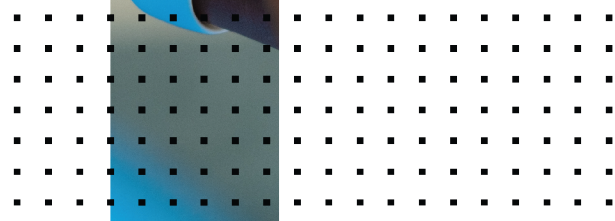
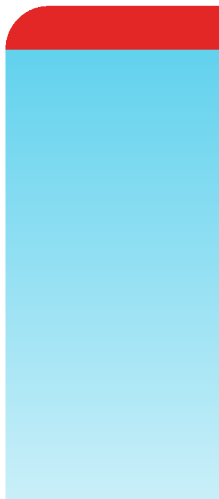


CLI Reference

FortiAnalyzer 7.0.10



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO LIBRARY

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/training-certification>

FORTINET TRAINING INSTITUTE

<https://training.fortinet.com>

FORTIGUARD LABS

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



October 26, 2023

FortiAnalyzer 7.0.10 CLI Reference

05-7010-686043-20231026

TABLE OF CONTENTS

Change Log	12
Introduction	13
FortiAnalyzer documentation	13
What's New in FortiAnalyzer 7.0	14
FortiAnalyzer 7.0.10	14
FortiAnalyzer 7.0.9	14
FortiAnalyzer 7.0.8	14
FortiAnalyzer 7.0.7	15
FortiAnalyzer 7.0.6	16
FortiAnalyzer 7.0.5	16
FortiAnalyzer 7.0.4	16
FortiAnalyzer 7.0.3	17
FortiAnalyzer 7.0.2	20
FortiAnalyzer 7.0.1	21
FortiAnalyzer 7.0.0	23
Using the Command Line Interface	27
CLI command syntax	27
Connecting to the CLI	28
Connecting to the FortiAnalyzer console	28
Setting administrative access on an interface	29
Connecting to the FortiAnalyzer CLI using SSH	29
Connecting to the FortiAnalyzer CLI using the GUI	30
CLI objects	30
CLI command branches	30
config branch	30
get branch	32
show branch	34
execute branch	35
diagnose branch	35
Example command sequences	35
CLI basics	36
Command help	36
Command tree	37
Command completion	37
Recalling commands	37
Editing commands	37
Line continuation	37
Command abbreviation	38
Environment variables	38
Encrypted password support	38
Entering spaces in strings	39
Entering quotation marks in strings	39
Entering a question mark (?) in a string	39

International characters	39
Special characters	39
IPv4 address formats	39
Changing the baud rate	40
Debug log levels	40
Administrative Domains	41
About ADOMs	41
Configuring ADOMs	42
system	43
admin	43
admin group	43
admin ldap	44
admin profile	46
admin radius	50
admin setting	51
admin tacacs	54
admin user	55
alert-console	62
alertemail	63
alert-event	64
auto-delete	66
backup all-settings	67
central-management	68
certificate	69
certificate ca	69
certificate crl	70
certificate local	71
certificate oftp	71
certificate remote	72
certificate ssh	72
connector	73
dns	74
docker	74
fips	75
fortiview	76
fortiview setting	76
fortiview auto-cache	76
global	77
Time zones	82
ha	84
interface	86
locallog	88
locallog setting	88
locallog disk setting	89
locallog filter	91
locallog fortianalyzer (fortianalyzer2, fortianalyzer3) setting	94

locallog memory setting	95
locallog syslogd (syslogd2, syslogd3) setting	96
log	97
log alert	97
log device-disable	98
fos-policy-stats	98
log interface-stats	99
log ioc	99
log mail-domain	100
log ratelimit	100
log settings	101
log topology	104
log-fetch	105
log-fetch client-profile	105
log-fetch server-setting	107
log-forward	107
log-forward-service	113
mail	114
metadata	115
ntp	116
password-policy	117
report	117
report auto-cache	117
report est-browse-time	118
report group	118
report setting	119
route	120
route6	121
saml	121
sniffer	123
snmp	124
snmp community	124
snmp sysinfo	127
snmp user	128
soc-fabric	130
sql	130
syslog	134
web-proxy	135
fmupdate	136
analyzer virusreport	136
av-ips	137
av-ips advanced-log	137
av-ips web-proxy	137
custom-url-list	138
disk-quota	139
fct-services	139

fds-setting	140
fds-setting push-override	142
fds-setting push-override-to-client	142
fds-setting server-override	143
fds-setting update-schedule	144
fwm-setting	144
multilayer	146
publicnetwork	147
server-access-priorities	147
server-override-status	148
service	149
web-spam	149
web-spam fgd-setting	149
web-spam web-proxy	153
fortirecorder	154
camera	154
camera devices	154
camera profile	161
camera video	162
global	163
schedule	164
execute	166
add-mgmt-license	166
add-on-license	167
add-vm-license	167
backup	168
bootimage	170
certificate	170
certificate ca	170
certificate crl	171
certificate local	171
certificate remote	173
console	173
console baudrate	173
date	174
device	174
erase-disk	175
factory-license	175
fmupdate	176
format	177
fortirecorder	177
iotop	178
iotps	179
log	179
log adom disk-quota	179

log device disk-quota	180
log device logstore	180
log device permissions	180
log device vdom	181
log dlp-files clear	181
log import	182
log ips-pkt clear	182
log quarantine-files clear	182
log storage-warning	183
log-aggregation	183
log-fetch	183
log-fetch client	183
log-fetch server	184
log-integrity	184
lvm	185
migrate	185
ping	186
ping6	186
raid	187
reboot	187
remove	188
reset	188
restore	189
sensor	191
shutdown	191
sql-local	191
sql-query-dataset	192
sql-query-generic	193
sql-report	193
ssh	196
ssh-known-hosts	196
tac	197
time	197
top	198
traceroute	199
traceroute6	199
diagnose	200
auto-delete	200
cdb	201
debug	202
debug application	202
debug backup-oldformat-script-logs	206
debug cdbchk	206
debug cli	206
debug console	207
debug coredump	207

debug crashlog	208
debug disable	208
debug enable	208
debug gui	208
debug info	209
debug klog	209
debug library	209
debug raw-elog	210
debug reset	210
debug service	210
debug sysinfo	211
debug sysinfo-log	211
debug sysinfo-log-backup	211
debug sysinfo-log-list	212
debug timestamp	212
debug vmd	212
debug vminfo	212
dlp-archives	213
docker	213
dvm	214
dvm adom	214
dvm capability	214
dvm chassis	215
dvm check-integrity	215
dvm csf	215
dvm dbstatus	216
dvm debug	216
dvm device	216
dvm device-tree-update	217
dvm extender	217
dvm fap	218
dvm fsw	218
dvm group	218
dvm lock	219
dvm proc	219
dvm remove	219
dvm supported-platforms	219
dvm task	220
dvm taskline	220
dvm transaction-flag	221
dvm workflow	221
faz-cdb	221
faz-cdb fix	221
faz-cdb reset	222
faz-cdb upgrade	222
fmnetwork	223
fmnetwork arp	223
fmnetwork interface	223
fmnetwork netstat	223

fmupdate	224
fortilogd	228
fortirecorder	229
fwmanager	229
ha	231
hardware	232
incident	232
license	232
log	233
pm2	233
report	233
rtm	234
siem	234
sniffer	234
sql	238
sql config	238
sql debug	239
sql hcache	240
sql process	242
sql remove	243
sql show	243
sql status	243
sql upload	244
svctools	244
system	245
system admin-session	245
system disk	246
system export	247
system flash	248
system fsck	248
system geoip	249
system geoip-city	249
system interface	249
system mapserver	250
system ntp	250
system print	250
system process	251
system raid	252
system route	252
system route6	253
system server	253
test	253
test application	253
test connection	263
test policy-check	264
test search	264
test sftp	264

upload	265
upload clear	265
upload status	265
vpn	266
get	267
fmupdate analyzer	268
fmupdate av-ips	268
fmupdate custom-url-list	268
fmupdate disk-quota	269
fmupdate fct-services	269
fmupdate fds-setting	269
fmupdate fwm-setting	270
fmupdate multilayer	271
fmupdate publicnetwork	271
fmupdate server-access-priorities	271
fmupdate server-override-status	271
fmupdate service	272
fmupdate web-spam	272
fortirecorder camera	272
fortirecorder global	273
fortirecorder schedule	273
system admin	274
system alert-console	275
system alertemail	275
system alert-event	275
system auto-delete	276
system backup	276
system central-management	276
system certificate	277
system connector	278
system dns	278
system docker	279
system fips	279
system fortiview	280
system global	280
system ha	281
system interface	282
system locallog	282
system log	283
system log-fetch	284
system log-forward	285
system log-forward-service	285
system loglimits	285
system mail	286

system metadata	286
system ntp	287
system password-policy	287
system performance	287
system report	288
system route	288
system route6	289
system saml	289
system sniffer	290
system snmp	290
system-soc-fabric	290
system sql	291
system status	292
system syslog	293
system web-proxy	293
show	295
Appendix A - Object Tables	296
Global object categories	296
Device object ID values	297
Appendix B - CLI Error Codes	300

Change Log

Date	Change Description
2023-10-26	Initial release.

Introduction

FortiAnalyzer offers centralized network security logging and reporting for the Fortinet Security Fabric. It provides a consolidated view across Fortinet devices throughout your organization with real-time alerts that expedite the discovery, investigation, and response to incidents even as they're happening. With action-oriented views and deep drill-down capabilities, FortiAnalyzer gives organizations critical insight into threats across the entire attack surface. It also provides real-time threat intelligence and actionable analytics via global IOC feeds to check for emerging and recent threats throughout the organization.

FortiAnalyzer includes:

- Centralized logging, reporting and event correlation
- Powerful NOC/SOC dashboard
- Automated indicators of compromise (IOC)
- Real-time and historical views into network activity

FortiAnalyzer documentation

The following FortiAnalyzer product documentation is available:

- *FortiAnalyzer Administration Guide*
This document describes how to set up the FortiAnalyzer system and use it with supported Fortinet units.
- *FortiAnalyzer device QuickStart Guides*
These documents are included with your FortiAnalyzer system package. Use this document to install and begin working with the FortiAnalyzer system and FortiAnalyzer GUI.
- *FortiAnalyzer Online Help*
You can get online help from the FortiAnalyzer GUI. FortiAnalyzer online help contains detailed procedures for using the FortiAnalyzer GUI to configure and manage FortiGate units.
- *FortiAnalyzer CLI Reference*
This document describes how to use the FortiAnalyzer Command Line Interface (CLI) and contains references for all FortiAnalyzer CLI commands.
- *FortiAnalyzer Release Notes*
This document describes new features and enhancements in the FortiAnalyzer system for the release, and lists resolved and known issues. This document also defines supported platforms and firmware versions.
- *FortiAnalyzer VM Install Guide*
This document describes installing FortiAnalyzer VM in your virtual environment.

What's New in FortiAnalyzer 7.0

The following tables list the commands and variables that have changed in the CLI.

FortiAnalyzer 7.0.10

The table below lists commands that have changed in version 7.0.10.

Command	Change
<code>config fmupdate fwm-setting</code>	Variables added: <ul style="list-style-type: none">• <code>retry-interval</code>• <code>retry-max</code>
<code>config fmupdate web-spam fgd-setting</code>	Variable added: <ul style="list-style-type: none">• <code>stat-log</code>
<code>config system log setting</code>	Variables added: <ul style="list-style-type: none">• <code>device-auto-detect</code>• <code>unencrypted-logging</code>
<code>diagnose debug raw-elog</code>	Command added.
<code>execute remove gui-data-cache</code>	Command added.

FortiAnalyzer 7.0.9

The table below lists commands that have changed in version 7.0.9.

Command	Change
<code>config system locallog [disk memory fortianalyzer fortianalyzer2 fortianalyzer3 syslogd syslogd2 syslogd3] filter</code>	Variable added: <ul style="list-style-type: none">• <code>controller</code>
<code>diagnose dvm remove autoupdate-log</code>	Command added.
<code>diagnose dvm supported-platforms fimg-list</code>	Command added.

FortiAnalyzer 7.0.8

The table below lists commands that have changed in version 7.0.8.

Command	Change
<code>config system global</code>	Variable added: <ul style="list-style-type: none"> no-copy-permission-check
<code>config system report auto-cache</code>	Variable added: <ul style="list-style-type: none"> sche-rpt-only
<code>diagnose docker upgrade</code>	Command updated.
<code>diagnose sql debug</code>	Commands added: <ul style="list-style-type: none"> pglog show pglog upload
<code>diagnose sql remove</code>	Command updated.

FortiAnalyzer 7.0.7

The table below lists commands that have changed in version 7.0.7.

Command	Change
<code>config fmupdate fds-setting</code>	Variable added: <ul style="list-style-type: none"> system-support-faz
<code>config system admin setting</code>	Variable added: <ul style="list-style-type: none"> fsw-ignore-platform-check
<code>config system global</code>	Variable added: <ul style="list-style-type: none"> gui-curl-timeout
<code>config system mail</code>	Variable added: <ul style="list-style-type: none"> from
<code>diagnose dvm adom</code>	Command added: <ul style="list-style-type: none"> reset-default-flags
<code>diagnose fwmanager</code>	Commands added: <ul style="list-style-type: none"> image-clear profile Commands updated: <ul style="list-style-type: none"> fwm-log set-controller-schedule
<code>diagnose ha</code>	Commands added: <ul style="list-style-type: none"> request-init-sync trace-client-req
<code>diagnose system disk</code>	Command added: <ul style="list-style-type: none"> delete

FortiAnalyzer 7.0.6

No commands have changed in FortiAnalyzer 7.0.6.

FortiAnalyzer 7.0.5

The table below lists commands that have changed in version 7.0.5.

Command	Change
<code>config fmupdate fwm-setting</code>	Command added: <ul style="list-style-type: none"> • upgrade-timeout
<code>config system global</code>	Variable added: <ul style="list-style-type: none"> • contentpack-fgt-install • gui-polling-interval
<code>config system ha</code>	Variable added: <ul style="list-style-type: none"> • hb-interface Command added: <ul style="list-style-type: none"> • vip
<code>diagnose cdb check</code>	Command added: <ul style="list-style-type: none"> • internet-service-name
<code>diagnose docker</code>	Command updated: <ul style="list-style-type: none"> • upgrade
<code>diagnose dvm supported-platforms</code>	Command updated: <ul style="list-style-type: none"> • fortiswitch
<code>diagnose sql remove</code>	Command updated: <ul style="list-style-type: none"> • hcache
<code>diagnose system print</code>	Command updated: <ul style="list-style-type: none"> • connector
<code>diagnose system process</code>	Command added: <ul style="list-style-type: none"> • fdlist
<code>execute fmupdate</code>	Command updated

FortiAnalyzer 7.0.4

The table below lists commands that have changed in version 7.0.4.

Command	Change
<code>config system admin profile</code>	Variable added: <ul style="list-style-type: none"> • device-fortixtender
<code>config system admin user</code>	Variable added: <ul style="list-style-type: none"> • fingerprint
<code>config system global</code>	Variable added: <ul style="list-style-type: none"> • table-entry-blink
<code>config system report setting</code>	Variable added: <ul style="list-style-type: none"> • max-rpt-pdf-rows
<code>config system syslog</code>	Variables added: <ul style="list-style-type: none"> • local-cert • peer-cert-cn • reliable • secure-connection
<code>diagnose docker upgrade</code>	Command updated
<code>diagnose dvm extender</code>	Command added: <ul style="list-style-type: none"> • import-profile
<code>diagnose fmnetwork interface</code>	Commands updated: <ul style="list-style-type: none"> • list • detail
<code>diagnose fwmanager</code>	Commands updated: <ul style="list-style-type: none"> • show-dev-upgrade-path • fwm-log
<code>diagnose ha</code>	Command added: <ul style="list-style-type: none"> • logs
<code>diagnose svctools import</code>	Commands updated: <ul style="list-style-type: none"> • local name • remote
<code>execute lvm</code>	Command removed: <ul style="list-style-type: none"> • start

FortiAnalyzer 7.0.3

The table below lists commands that have changed in version 7.0.3.

Command	Change
<code>config system admin ldap</code>	Variable added: <ul style="list-style-type: none"> • adom-access

Command	Change
<code>config system admin profile</code>	Variables added: <ul style="list-style-type: none"> • rpc-permit • trusthost1 • trusthost2 • trusthost3 • trusthost4 • trusthost5 • trusthost6 • trusthost7 • trusthost8 • trusthost9 • trusthost10 • ipv6_trusthost1 • ipv6_trusthost2 • ipv6_trusthost3 • ipv6_trusthost4 • ipv6_trusthost5 • ipv6_trusthost6 • ipv6_trusthost7 • ipv6_trusthost8 • ipv6_trusthost9 • ipv6_trusthost10 Variable removed: <ul style="list-style-type: none"> • ips-baseline-ovrd
<code>config system admin setting</code>	Variable added: <ul style="list-style-type: none"> • idle_timeout_sso
<code>config system admin user</code>	Variables added: <ul style="list-style-type: none"> • adom-access • th-from-profile • th6-from-profile Variable removed: <ul style="list-style-type: none"> • adom-exclude
<code>config system fortiview setting</code>	Variable added: <ul style="list-style-type: none"> • data-source
<code>config system global</code>	Variable added: <ul style="list-style-type: none"> • normalized-intf-zone-only
<code>config system ha</code>	Variable added: <ul style="list-style-type: none"> • cfg-sync-hb-interval
<code>config system locallog disk setting</code>	Variable added:

Command	Change
	<ul style="list-style-type: none"> log-disk-quota
<code>config system locallog {fortianalyzer fortianalyzer2 fortianalyzer3} setting</code>	Variable added: <ul style="list-style-type: none"> peer-cert-cn
<code>config system log ratelimit</code>	Subcommand renamed and updated: <ul style="list-style-type: none"> device to ratelimits
<code>config system log settings</code>	Subcommands updated: <ul style="list-style-type: none"> rolling-analyzer rolling-local rolling-regular
<code>config system log-fetch client-profile</code>	Variable added: <ul style="list-style-type: none"> peer-cert-cn
<code>config system log-forward</code>	Subcommand updated: <ul style="list-style-type: none"> device-filter Variables added: <ul style="list-style-type: none"> agg-data-end-time agg-data-start-time agg-schedule pcapurl-domain-ip pcapurl-enrich peer-cert-cn
<code>config system ntp</code>	Subcommand updated: <ul style="list-style-type: none"> ntpserver Variable removed: <ul style="list-style-type: none"> sync_interval
<code>config system web-proxy</code>	Command added
<code>config system workflow</code>	Command removed
<code>diagnose debug application</code>	Commands removed: <ul style="list-style-type: none"> ntpd sql-dashboard-rpt
<code>diagnose docker upgrade</code>	Command updated
<code>diagnose fmupdate</code>	Command added: <ul style="list-style-type: none"> dump-um-db Command updated: <ul style="list-style-type: none"> fgt-del-um-db
<code>diagnose rtm</code>	Command added
<code>diagnose system print</code>	Command removed: <ul style="list-style-type: none"> certificate

Command	Change
<code>execute remove endpoints-endusers</code>	Command added

FortiAnalyzer 7.0.2

The table below lists commands that have changed in version 7.0.2.

Command	Change
<code>config system admin setting</code>	Variable added: <ul style="list-style-type: none"> • preferred-fgfm-intf
<code>config system connector</code>	Variable renamed: <ul style="list-style-type: none"> • px-refresh-interval to conn-refresh-interval
<code>config system docker</code>	Variables removed: <ul style="list-style-type: none"> • fortiaiops • fortiauthenticator • fortiportal • fortisigconverter • fortiwlm • sdwancontroller • universalconnector
<code>config system global</code>	Command added: <ul style="list-style-type: none"> • ssl-cipher-suites
<code>config system locallog disk setting</code>	Variable added: <ul style="list-style-type: none"> • max-log-file-num
<code>config system log</code>	Command added: <ul style="list-style-type: none"> • fos-policy-stats • topology
<code>config system log-forward</code>	Variable added: <ul style="list-style-type: none"> • fwd-ha-bind-vip
<code>config system log settings</code>	Variable added: <ul style="list-style-type: none"> • keep-dev-logs
<code>diagnose debug application</code>	Commands added: <ul style="list-style-type: none"> • archd • fgdlinkd
<code>diagnose docker</code>	Commands updated: <ul style="list-style-type: none"> • reset • upgrade

Command	Change
<code>diagnose fmupdate</code>	Command added: <ul style="list-style-type: none"> • <code>fgd-dump</code> Commands removed: <ul style="list-style-type: none"> • <code>fct-getobject</code> • <code>fds-get-downstream-device</code> • <code>fgd-asdevice-stat</code> • <code>fgd-asserver-stat</code> • <code>fgd-get-downstream-device</code> • <code>get-device</code> Commands updated: <ul style="list-style-type: none"> • <code>del-device</code> • <code>updatenow</code>
<code>diagnose fwmanager</code>	Commands removed: <ul style="list-style-type: none"> • <code>cancel-schedule</code> • <code>get-all-schedule</code> • <code>get-dev-schedule</code> • <code>get-grp-schedule</code>
<code>diagnose sql config</code>	Commands added: <ul style="list-style-type: none"> • <code>hcache-max-base-row</code> • <code>hcache-max-fv-row-per-timescale</code>
<code>diagnose test application</code>	Command added: <ul style="list-style-type: none"> • <code>archd</code>
<code>execute migrate fabric</code>	Command added
<code>execute tac cleanup</code>	Command added

FortiAnalyzer 7.0.1

The table below lists commands that have changed in version 7.0.1.

Command	Change
<code>config fmupdate fds-setting</code>	Variables added: <ul style="list-style-type: none"> • <code>system-support-fdc</code> • <code>system-support-fts</code> Variable removed: <ul style="list-style-type: none"> • <code>system-support-fsw</code>
<code>config fmupdate fwm-setting</code>	Variable added: <ul style="list-style-type: none"> • <code>log</code>

Command	Change
<code>config fmupdate web-spam fgd-setting</code>	Variables added: <ul style="list-style-type: none"> • <code>iot-cache</code> • <code>iot-log</code> • <code>iot-preload</code> • <code>restrict-iots-dbver</code>
<code>config system admin profile</code>	Variable added: <ul style="list-style-type: none"> • <code>ips-baseline-ovrd</code>
<code>config system admin setting</code>	Variables added: <ul style="list-style-type: none"> • <code>auth-addr</code> • <code>auth-port</code>
<code>config system docker</code>	Variables added: <ul style="list-style-type: none"> • <code>fortiaios</code> • <code>fsmcollector</code> • <code>universalconnector</code>
<code>config system locallog {syslogd syslogd2 syslogd3} setting</code>	Variables added: <ul style="list-style-type: none"> • <code>cert</code> • <code>reliable</code> • <code>secure-connection</code>
<code>config system saml</code>	Variable added: <ul style="list-style-type: none"> • <code>user-auto-create</code>
<code>diagnose docker</code>	Command added: <ul style="list-style-type: none"> • <code>reset</code> Command updated: <ul style="list-style-type: none"> • <code>upgrade</code>
<code>diagnose faz-cdb fix</code>	Command added
<code>diagnose fmupdate</code>	Commands added: <ul style="list-style-type: none"> • <code>crdb</code> • <code>priority-download</code>
<code>diagnose fortilogd lograte-device</code>	Command updated
<code>diagnose ha</code>	Command renamed: <ul style="list-style-type: none"> • <code>dbhash</code> to <code>check-data</code> Command renamed and updated: <ul style="list-style-type: none"> • <code>dbhash-report</code> to <code>data-check-report</code>
<code>diagnose system disk</code>	Command added: <ul style="list-style-type: none"> • <code>usage</code>
<code>diagnose system print</code>	Command updated: <ul style="list-style-type: none"> • <code>df</code>

Command	Change
<code>execute certificate</code>	Command added: <ul style="list-style-type: none"> • <code>crl</code>
<code>execute certificate ca</code>	Command updated: <ul style="list-style-type: none"> • <code>import</code>
<code>execute certificate local</code>	Command updated: <ul style="list-style-type: none"> • <code>import</code>
<code>execute fmupdate</code>	Command added: <ul style="list-style-type: none"> • <code>fgd-db-merge</code>
<code>execute migrate</code>	Command added: <ul style="list-style-type: none"> • <code>serial-number-list</code>
<code>execute restore image {scp sftp}</code>	Command added

FortiAnalyzer 7.0.0

The table below lists commands that have changed in version 7.0.0.

Command	Change
<code>config system admin profile</code>	Variables added: <ul style="list-style-type: none"> • <code>execute-playbook</code> • <code>extension-access</code> • <code>fabric-viewer</code> • <code>run-report</code> • <code>script-access</code> • <code>triage-events</code> • <code>update-incidents</code>
<code>config system admin setting</code>	Variables added: <ul style="list-style-type: none"> • <code>idle_timeout_api</code> • <code>idle_timeout_gui</code>
<code>config system admin user</code>	Variables added: <ul style="list-style-type: none"> • <code>login-max</code> • <code>use-global-theme</code> • <code>user-theme</code>
<code>config system docker</code>	Variables added: <ul style="list-style-type: none"> • <code>docker-user-login-max</code> • <code>fortisoar</code>
<code>config system global</code>	Variables added: <ul style="list-style-type: none"> • <code>object-revision-db-max</code>

Command	Change
	<ul style="list-style-type: none"> object-revision-mandatory-note object-revision-object-max object-revision-status
<code>config system interface</code>	Variables added: <ul style="list-style-type: none"> aggregate lacp-mode lacp-speed link-up-delay min-links min-links-down type Subcommand added: <ul style="list-style-type: none"> member
<code>config system log</code>	Command added: <ul style="list-style-type: none"> ratelimit
<code>config system log-forward</code>	Variables added: <ul style="list-style-type: none"> fwd-compression log-masking-custom-priority log-masking-fields log-masking-key log-masking-status Variable renamed: <ul style="list-style-type: none"> server-ip to server-addr Subcommand added: <ul style="list-style-type: none"> log-masking-custom
<code>config system mail</code>	Variables added: <ul style="list-style-type: none"> auth-type local-cert
<code>config system saml</code>	Variable added: <ul style="list-style-type: none"> forticloud-sso
<code>config system soc-fabric</code>	Command added
<code>diagnose debug application</code>	Command added: <ul style="list-style-type: none"> fabricsyncd
<code>diagnose docker upgrade</code>	Command updated
<code>diagnose dvm debug</code>	Command added: <ul style="list-style-type: none"> trace
<code>diagnose dvm extender</code>	Command removed: <ul style="list-style-type: none"> import-dataplan-to-adom

Command	Change
	Commands renamed and updated: <ul style="list-style-type: none"> import-sim-profile-to-adom to import-template set-sim-profile to set-template
diagnose fmupdate check-disk-quota	Command updated
diagnose fwmanager	Command added: <ul style="list-style-type: none"> image-delete Commands removed: <ul style="list-style-type: none"> delete-all delete-imported-images delete-official-images delete-serverlist imported-imagelist reset-schedule-database serverlist Command renamed: <ul style="list-style-type: none"> download-image to image-download Command renamed and updated: <ul style="list-style-type: none"> official-imagelist to image-list Command updated: <ul style="list-style-type: none"> fwm-log
diagnose ha	Commands added: <ul style="list-style-type: none"> dbhash action dbhash-report
diagnose siem process	Command added
diagnose sql debug hcache-aggr	Command updated: <ul style="list-style-type: none"> show
diagnose sql debug logview	Command added
diagnose sql debug sqlqry	Command updated: <ul style="list-style-type: none"> show
diagnose system export	Commands updated: <ul style="list-style-type: none"> crashlog upgradelog vartmp
diagnose test application	Command added: <ul style="list-style-type: none"> fabricsyncd

Command	Change
<code>execute tac</code>	Command updated: <ul style="list-style-type: none">• report Command added: <ul style="list-style-type: none">• upload

Using the Command Line Interface

This chapter explains how to connect to the CLI and describes the basics of using the CLI. You can use CLI commands to view all system information and to change all system configuration settings.

This chapter describes:

- CLI command syntax
- Connecting to the CLI
- CLI objects
- CLI command branches
- CLI basics

CLI command syntax

This guide uses the following conventions to describe command syntax.

- Angle brackets < > indicate variables.
- Vertical bar and curly brackets { | } separate alternative, mutually exclusive required keywords.

For example:

```
set protocol {ftp | sftp}
```

You can enter `set protocol ftp` or `set protocol sftp`.

- Square brackets [] indicate that a variable is optional.

For example:

```
show system interface [<name_str>]
```

To show the settings for all interfaces, you can enter `show system interface`. To show the settings for the Port1 interface, you can enter `show system interface port1`.

- A space separates options that can be entered in any combination and must be separated by spaces.

For example:

```
set allowaccess {fgfm http https https-logging ping snmp soc-fabric ssh webservice}
```

You can enter any of the following:

```
set allowaccess ping
```

```
set allowaccess https ping
```

```
set allowaccess fgfm http https https-logging ping snmp soc-fabric ssh webservice
```

In most cases to make changes to lists that contain options separated by spaces, you need to retype the whole list including all the options you want to apply and excluding all the options you want to remove.

- Special characters:
 - The \ is supported to escape spaces or as a line continuation character.
 - The single quotation mark ' and the double quotation mark " are supported, but must be used in pairs.
 - If there are spaces in a string, you must precede the spaces with the \ escape character or put the string in a pair of quotation marks.

Connecting to the CLI

You can use a direct console connection, SSH, or the CLI console widget in the GUI to connect to the FortiAnalyzer CLI. For more information, see the [FortiAnalyzer Administration Guide](#) and your device's [QuickStart Guide](#).

- [Connecting to the FortiAnalyzer console](#)
- [Setting administrative access on an interface](#)
- [Connecting to the FortiAnalyzer CLI using SSH](#)
- [Connecting to the FortiAnalyzer CLI using the GUI](#)

Connecting to the FortiAnalyzer console

To connect to the FortiAnalyzer console, you need:

- a computer with an available communications port
- a console cable, provided with your FortiAnalyzer unit, to connect the FortiAnalyzer console port to a communications port on your computer
- terminal emulation software, such as HyperTerminal for Windows.



The following procedure describes how to connect to the FortiAnalyzer CLI using Windows HyperTerminal software. You can use any terminal emulation program.

To connect to the CLI:

1. Connect the FortiAnalyzer console port to the available communications port on your computer.
2. Make sure that the FortiAnalyzer unit is powered on.
3. Start a terminal emulation program on the management computer, select the COM port, and use the following settings:

COM port	COM1
Baud rate	9600
Data bits	8
Parity	None
Stop bits	1
Flow control	None

4. Press `Enter` to connect to the FortiAnalyzer CLI.
5. In the log in prompt, enter the username and password.
The default log in is username: `admin`, and no password.
You have connected to the FortiAnalyzer CLI, and you can enter CLI commands.

Setting administrative access on an interface

To perform administrative functions through a FortiAnalyzer network interface, you must enable the required types of administrative access on the interface to which your management computer connects. Access to the CLI requires Secure Shell (SSH) access. If you want to use the GUI, you need HTTPS access.

To use the GUI to configure FortiAnalyzer interfaces for SSH access, see the [FortiAnalyzer Administration Guide](#).

To use the CLI to configure SSH access:

1. Connect and log into the CLI using the FortiAnalyzer console port and your terminal emulation software.
2. Use the following command to configure an interface to accept SSH connections:

```
config system interface
  edit <interface_name>
    set allowaccess <access_types>
  end
```

Where `<interface_name>` is the name of the FortiAnalyzer interface to be configured to allow administrative access, and `<access_types>` is a whitespace-separated list of access types to enable.

For example, to configure port1 to accept HTTPS and SSH connections, enter:

```
config system interface
  edit port1
    set allowaccess https ssh
  end
```



Remember to press `Enter` at the end of each line in the command example. Also, type `end` and press `Enter` to commit the changes to the FortiAnalyzer configuration.

3. To confirm that you have configured SSH access correctly, enter the following command to view the access settings for the interface:

```
get system interface <interface_name>
```

The CLI displays the settings, including the management access settings, for the named interface.

Connecting to the FortiAnalyzer CLI using SSH

SSH provides strong secure authentication and secure communications to the FortiAnalyzer CLI from your internal network or the internet. Once the FortiAnalyzer unit is configured to accept SSH connections, you can run an SSH client on your management computer and use this client to connect to the FortiAnalyzer CLI.

To connect to the CLI using SSH:

1. Install and start an SSH client.
2. Connect to a FortiAnalyzer interface that is configured for SSH connections.
3. Type a valid administrator name and press `Enter`.
4. Type the password for this administrator and press `Enter`.
The FortiAnalyzer model name followed by a # is displayed.
You have connected to the FortiAnalyzer CLI, and you can enter CLI commands.

Connecting to the FortiAnalyzer CLI using the GUI

The GUI also provides a CLI console widget.

To connect to the CLI using the GUI:

1. Connect to the GUI and log in.
For information about how to do this, see the [FortiAnalyzer Administration Guide](#).
2. From the *Tools* dropdown in the banner, click *>_ CLI Console*.
The *CLI Console* widget opens.

CLI objects

The FortiAnalyzer CLI is based on configurable objects. The top-level objects are the basic components of FortiAnalyzer functionality.

system	Configuration options related to the overall operation of the FortiAnalyzer unit, such as interfaces, virtual domains, and administrators.
fmupdate	Configures settings related to FortiGuard service updates and the unit's built-in FDS.

This object contains more specific lower level objects. For example, the system object contains objects for administrators, DNS, interfaces and so on.

CLI command branches

The FortiAnalyzer CLI consists of the following command branches:

config branch	execute branch
get branch	diagnose branch
show branch	

Examples showing how to enter command sequences within each branch are provided in the following sections.

config branch

The `config` commands configure objects of FortiAnalyzer functionality. Top-level objects are not configurable, they are containers for more specific lower level objects. For example, the system object contains administrators, DNS addresses, interfaces, routes, and so on. When these objects have multiple sub-objects, such as administrators or routes, they are organized in the form of a table. You can add, delete, or edit the entries in the table. Table entries each consist of variables that you can set to particular values. Simpler objects, such as system DNS, are a single set of variables.

To configure an object, you use the `config` command to navigate to the object's command "shell". For example, to configure administrators, you enter the command

```
config system admin user
```

The command prompt changes to show that you are in the admin shell.

```
(user) #
```

This is a table shell. You can use any of the following commands:

edit	Add an entry to the FortiAnalyzer configuration or edit an existing entry. For example in the <code>config system admin shell</code> : <ul style="list-style-type: none"> Type <code>edit admin</code> and press <code>Enter</code> to edit the settings for the default admin administrator account. Type <code>edit newadmin</code> and press <code>Enter</code> to create a new administrator account with the name <code>newadmin</code> and to edit the default settings for the new administrator account.
delete	Remove an entry from the FortiAnalyzer configuration. For example in the <code>config system admin shell</code> , type <code>delete newadmin</code> and press <code>Enter</code> to delete the administrator account named <code>newadmin</code> .
purge	Remove all entries configured in the current shell. For example in the <code>config user local shell</code> : <ul style="list-style-type: none"> Type <code>get</code> to see the list of user names added to the FortiAnalyzer configuration, Type <code>purge</code> and then <code>y</code> to confirm that you want to purge all the user names, Type <code>get</code> again to confirm that no user names are displayed.
get	List the configuration. In a table shell, <code>get</code> lists the table members. In an edit shell, <code>get</code> lists the variables and their values.
show	Show changes to the default configuration as configuration commands.
end	Save the changes you have made in the current shell and leave the shell. Every <code>config</code> command must be paired with an <code>end</code> command. You will return to the root FortiAnalyzer CLI prompt. The <code>end</code> command is also used to save <code>set</code> command changes and leave the shell.

If you enter the `get` command, you see a list of the entries in the table of administrators. To add a new administrator, you enter the `edit` command with a new administrator name:

```
edit admin_1
```

The FortiAnalyzer unit acknowledges the new table entry and changes the command prompt to show that you are now editing the new entry:

```
new entry 'admin_1' added
(admin_1) #
```

From this prompt, you can use any of the following commands:

config	In a few cases, there are subcommands that you access using a second <code>config</code> command while editing a table entry. An example of this is the command to add restrict the user to specific devices or VDOMs.
set	Assign values. For example from the <code>edit admin</code> command shell, typing <code>set password newpass</code> changes the password of the admin administrator account to <code>newpass</code> .

	When using a <code>set</code> command to make changes to lists that contain options separated by spaces, you need to retype the whole list including all the options you want to apply and excluding all the options you want to remove.
unset	Reset values to defaults. For example from the <code>edit admin</code> command shell, typing <code>unset password</code> resets the password of the admin administrator account to the default of no password.
get	List the configuration. In a table shell, <code>get</code> lists the table members. In an edit shell, <code>get</code> lists the variables and their values.
show	Show changes to the default configuration in the form of configuration commands.
next	Save the changes you have made in the current shell and continue working in the shell. For example if you want to add several new admin user accounts enter the <code>config system admin user shell</code> . <ul style="list-style-type: none"> • Type <code>edit User1</code> and press <code>Enter</code>. • Use the <code>set</code> commands to configure the values for the new admin account. • Type <code>next</code> to save the configuration for User1 without leaving the <code>config system admin user shell</code>. • Continue using the <code>edit</code>, <code>set</code>, and <code>next</code> commands to continue adding admin user accounts. • Type <code>end</code> and press <code>Enter</code> to save the last configuration and leave the shell.
abort	Exit an edit shell without saving the configuration.
end	Save the changes you have made in the current shell and leave the shell. Every <code>config</code> command must be paired with an <code>end</code> command. The <code>end</code> command is also used to save <code>set</code> command changes and leave the shell.

The `config` branch is organized into configuration shells. You can complete and save the configuration within each shell for that shell, or you can leave the shell without saving the configuration. You can only use the configuration commands for the shell that you are working in. To use the configuration commands for another shell you must leave the shell you are working in and enter the other shell.

get branch

Use `get` to display settings. You can use `get` within a `config` shell to display the settings for that shell, or you can use `get` with a full path to display the settings for the specified shell.

To use `get` from the root prompt, you must include a path to a shell.

The root prompt is the FortiAnalyzer host or model name followed by a number sign (#).

Example 1

When you type `get` in the `config system admin user shell`, the list of administrators is displayed.

At the `(user) #` prompt, type:

```
get
```

The screen displays:

```
== [ admin ]
userid: admin
== [ admin2 ]
```



```
userid: admin2
== [ admin3 ]
userid: admin3
```

Example 2

When you type `get` in the `admin` user shell, the configuration values for the admin administrator account are displayed.

```
edit admin
```

At the `(admin) #` prompt, type:

```
get
```

The screen displays:

```
userid : admin
login-max : 32
password : *
change-password : enable
trusthost1 : 0.0.0.0 0.0.0.0
trusthost2 : 255.255.255.255 255.255.255.255
trusthost3 : 255.255.255.255 255.255.255.255
trusthost4 : 255.255.255.255 255.255.255.255
trusthost5 : 255.255.255.255 255.255.255.255
trusthost6 : 255.255.255.255 255.255.255.255
trusthost7 : 255.255.255.255 255.255.255.255
trusthost8 : 255.255.255.255 255.255.255.255
trusthost9 : 255.255.255.255 255.255.255.255
trusthost10 : 255.255.255.255 255.255.255.255
ipv6_trusthost1 : ::/0
ipv6_trusthost2 : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128
ipv6_trusthost3 : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128
ipv6_trusthost4 : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128
ipv6_trusthost5 : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128
ipv6_trusthost6 : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128
ipv6_trusthost7 : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128
ipv6_trusthost8 : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128
ipv6_trusthost9 : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128
ipv6_trusthost10 : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128
profileid : Super_User
dev-group : (null)
description : (null)
user_type : local
ssh-public-key1 :
ssh-public-key2 :
ssh-public-key3 :
avatar : (null)
meta-data:
  == [ Contact Email ]
  fieldname: Contact Email
  == [ Contact Phone ]
  fieldname: Contact Phone
password-expire : 0000-00-00 00:00:00
force-password-change: disable
rpc-permit : none
use-global-theme : enable
last-name : (null)
first-name : (null)
```

```
email-address : (null)
phone-number  : (null)
mobile-number : (null)
pager-number  : (null)
hidden       : 0
dashboard-tabs:
dashboard:
```

Example 3

You want to confirm the IP address and netmask of the port1 interface from the root prompt.

At the (command) # prompt, type:

```
get system interface port1
```

The screen displays:

```
name : port1
status : enable
ip : *.*.*.*.* 255.255.255.0
allowaccess : https ssh
speed : auto
description : (null)
alias : (null)
mtu : 1500
type : physical
ipv6:
  ip6-address: ::/0 ip6-allowaccess: ip6-autoconf: enable
```

show branch

Use `show` to display the FortiAnalyzer unit configuration. Only changes to the default configuration are displayed. You can use `show` within a `config` shell to display the configuration of that shell, or you can use `show` with a full path to display the configuration of the specified shell.

To display the configuration of all `config` shells, you can use `show` from the root prompt. The root prompt is the FortiAnalyzer host or model name followed by a number sign (#).

Example 1

When you type `show` and press `Enter` within the `port1` interface shell, the changes to the default interface configuration are displayed.

At the (port1) # prompt, type:

```
show
```

The screen displays:

```
config system interface
  edit "port1"
    set ip *.*.*.*.* 255.255.255.0
    set allowaccess https ssh
  next
end
```

Example 2

You are working in the `port1` interface shell and want to see the `system dns` configuration. At the `(port1) #` prompt, type:

```
show system dns
```

The screen displays:

```
config system dns
  set primary 65.39.139.53
  set secondary 65.39.139.63
end
```

execute branch

Use `execute` to run static commands, to reset the FortiAnalyzer unit to factory defaults, or to back up or restore the FortiAnalyzer configuration. The execute commands are available only from the root prompt.

The root prompt is the FortiAnalyzer host or model name followed by a number sign (#).

Example

At the root prompt, type:

```
execute reboot
The system will be rebooted.
Do you want to continue? (y/n)
```

and press `Enter` to restart the FortiAnalyzer unit.

diagnose branch

Commands in the `diagnose` branch are used for debugging the operation of the FortiAnalyzer unit and to set parameters for displaying different levels of diagnostic information.



Diagnose commands are intended for advanced users only. Contact Fortinet Technical Support before using these commands.

Example command sequences



The command prompt changes for each shell.

To configure the primary and secondary DNS server addresses:

1. Starting at the root prompt, type:
`config system dns`
and press `Enter`. The prompt changes to `(dns) #`.
2. At the `(dns) #` prompt, type (question mark) `?`
The following options are displayed.
`set`
`unset`
`get`
`show`
`abort`
`end`
3. Type `set` (question mark) `?`
The following options are displayed:
`primary`
`secondary`
`ip6-primary`
`ip6-secondary`
4. To set the primary DNS server address to `172.16.100.100`, type:
`set primary 172.16.100.100`
and press `Enter`.
5. To set the secondary DNS server address to `207.104.200.1`, type:
`set secondary 207.104.200.1`
and press `Enter`.
6. To restore the primary DNS server address to the default address, type `unset primary` and press `Enter`.
7. If you want to leave the `config system dns` shell without saving your changes, type `abort` and press `Enter`.
8. To save your changes and exit the `dns` sub-shell, type `end` and press `Enter`.
9. To confirm your changes have taken effect after leaving the `dns` sub-shell, type `get system dns` and press `Enter`.

CLI basics

This section covers command line interface basic information.

Command help

You can press the question mark (?) key to display command help.

- Press the question mark (?) key at the command prompt to display a list of the commands available and a description of each command.
- Enter a command followed by a space and press the question mark (?) key to display a list of the options available for that command and a description of each option.
- Enter a command followed by an option and press the question mark (?) key to display a list of additional options available for that command option combination and a description of each option.

Command tree

Enter `tree` to display the FortiAnalyzer CLI command tree. To capture the full output, connect to your device using a terminal emulation program, such as PuTTY, and capture the output to a log file. For `config` commands, use the `tree` command to view all available variables and sub-commands.

Command completion

You can use the tab key or the question mark (?) key to complete commands.

- You can press the tab key at any prompt to scroll through the options available for that prompt.
- You can type the first characters of any command and press the tab key or the question mark (?) key to complete the command or to scroll through the options that are available at the current cursor position.
- After completing the first word of a command, you can press the space bar and then the tab key to scroll through the options available at the current cursor position.

Recalling commands

You can recall previously entered commands by using the Up and Down arrow keys to scroll through commands you have entered.

Editing commands

Use the left and right arrow keys to move the cursor back and forth in a recalled command. You can also use Backspace and Delete keys, and the control keys listed in the following table to edit the command.

Function	Key combination
Beginning of line	Control key + A
End of line	Control key + E
Back one word	Control key + B
Forward one word	Control key + F
Delete current character	Control key + D
Previous command	Control key + P
Next command	Control key + N
Abort the command	Control key + C
If used at the root prompt, exit the CLI	Control key + C

Line continuation

To break a long command over multiple lines, use a `\` at the end of each line.

Command abbreviation

You can abbreviate commands and command options to the smallest number of non-ambiguous characters. For example, the command `get system status` can be abbreviated to `g sy st`.

Environment variables

The FortiAnalyzer CLI supports several environment variables.

\$USERFROM	The management access type (SSH, Telnet and so on) and the IPv4 address of the logged in administrator.
\$USERNAME	The user account name of the logged in administrator.
\$SerialNum	The serial number of the FortiAnalyzer unit.

Variable names are case sensitive. In the following example, when entering the variable, you can type `$` followed by a tab to auto-complete the variable to ensure that you have the exact spelling and case. Continue pressing tab until the variable you want to use is displayed.

```
config system global
  set hostname $SerialNum
end
```

Encrypted password support

After you enter a clear text password using the CLI, the FortiAnalyzer unit encrypts the password and stores it in the configuration file with the prefix `ENC`. For example:

```
show system admin user user1
config system admin user
  edit "user1"
    set password ENC
      UAGUDZ1yEaG30620s6afD3Gac1FnOT0BC1rVJmMFC9ubLlW4wEvHcqGVq+ZnrgbudK7aryyf1scXcX
      dnQxskRcU3E9XqOit82PgScwzGzGuJ5a9f
    set profileid "Standard_User"
  next
end
```

It is also possible to enter an already encrypted password. For example, type:

```
config system admin
```

then press `Enter`.

Enter:

```
edit user1
```

then press `Enter`.

Enter:

```
set password ENC
  UAGUDZ1yEaG30620s6afD3Gac1FnOT0BC1rVJmMFC9ubLlW4wEvHcqGVq+ZnrgbudK7aryyf1scXcXdnQxsk
  RcU3E9XqOit82PgScwzGzGuJ5a9f
```

then press `Enter`.

`Enter`:

`end`

then press `Enter`.

Entering spaces in strings

When a string value contains a space, do one of the following:

- Enclose the string in quotation marks, "Security Administrator", for example.
- Enclose the string in single quotes, 'Security Administrator', for example.
- Use a backslash ("\") preceding the space, Security\ Administrator, for example.

Entering quotation marks in strings

If you want to include a quotation mark, single quote, or apostrophe in a string, you must precede the character with a backslash character. To include a backslash, enter two backslashes.

Entering a question mark (?) in a string

If you want to include a question mark (?) in a string, you must precede the question mark with CTRL-V. Entering a question mark without first entering CTRL-V causes the CLI to display possible command completions, terminating the string.

International characters

The CLI supports international characters in strings.

Special characters

The characters <, >, (,), #, ', and " are not permitted in most CLI fields, but you can use them in passwords. If you use the apostrophe (') or quote (") character, you must precede it with a backslash (\) character when entering it in the CLI `set` command.

IPv4 address formats

You can enter an IPv4 address and subnet using either dotted decimal or slash-bit format. For example you can type either:

```
set ip 192.168.1.1 255.255.255.0
```

or

```
set ip 192.168.1.1/24
```

The IPv4 address is displayed in the configuration file in dotted decimal format.

Changing the baud rate

Using `execute console baudrate`, you can change the default console connection baud rate.



Changing the default baud rate is not available on all models.

Debug log levels

The following table lists available debug log levels on your FortiAnalyzer.

0	Emergency	The system has become unusable.
1	Alert	Immediate action is required.
2	Critical	Functionality is affected.
3	Error	An erroneous condition exists and functionality is probably affected.
4	Warning	Function might be affected.
5	Notice	Notification of normal events.
6	Information	General information about system operations.
7	Debug	Detailed information useful for debugging purposes.
8	Maximum	Maximum log level.

Administrative Domains

Administrative domains (ADOMs) enable the admin administrator to constrain other Fortinet unit administrators' access privileges to a subset of devices in the device list. For FortiGate devices with virtual domains (VDOMs), ADOMs can further restrict access to only data from a specific FortiGate VDOM.

About ADOMs

Enabling ADOMs alters the structure and available functionality of the GUI and CLI according to whether you are logging in as the `admin` administrator, and, if you are not logging in as the `admin` administrator, the administrator account's assigned access profile.



The `admin` administrator can further restrict other administrators' access to specific configuration areas within their ADOM by using access profiles .

Characteristics of the CLI and GUI when ADOMs are enabled

	Admin administrator account	Other administrators
Access to config system global	Yes	No
Can create administrator accounts	Yes	No
Can enter all ADOMs	Yes	No

- If ADOMs are enabled and you log in as `admin`, a superset of the typical CLI commands appear, allowing unrestricted access and ADOM configuration.
`config system global` contains settings used by the FortiAnalyzer unit itself and settings shared by ADOMs, such as the device list, RAID, and administrator accounts. It does not include ADOM-specific settings or data, such as logs and reports. When configuring other administrator accounts, an additional option appears allowing you to restrict other administrators to an ADOM.
- If ADOMs are enabled and you log in as any other administrator, you enter the ADOM assigned to your account. A subset of the typical menus or CLI commands appear, allowing access only to only logs, reports, quarantine files, content archives, IP aliases, and LDAP queries specific to your ADOM. You cannot access Global Configuration, or enter other ADOMs.
By default, administrator accounts other than the `admin` account are assigned to the `root` ADOM, which includes all devices in the device list. By creating ADOMs that contain a subset of devices in the device list, and assigning them to administrator accounts, you can restrict other administrator accounts to a subset of the FortiAnalyzer unit's total devices or VDOMs.

The `admin` administrator account cannot be restricted to an ADOM. Other administrators are restricted to their ADOM, and cannot configure ADOMs or Global Configuration.

The maximum number of ADOMs varies by FortiAnalyzer model.

Configuring ADOMs

To use administrative domains, the `admin` administrator must first enable the feature, create ADOMs, and assign existing FortiAnalyzer administrators to ADOMs.



Enabling ADOMs moves non-global configuration items to the `root` ADOM. Back up the FortiAnalyzer unit configuration before enabling ADOMs.

Within the CLI, you can enable ADOMs and set the administrator ADOM. To configure the ADOMs, you must use the GUI.

To enable or disable ADOMs:

Enter the following CLI command:

```
config system global
    set adom-status {enable | disable}
end
```

An administrative domain has two modes: normal and advanced. Normal mode is the default device mode. In normal mode, a FortiGate unit can only be added to a single administrative domain. In advanced mode, you can assign different VDOMs from the same FortiGate to multiple administrative domains.



Enabling the advanced mode option will result in more complicated management scenarios. It is recommended only for advanced users.

To change ADOM device modes:

Enter the following CLI command:

```
config system global
    set adom-mode {advanced | normal}
end
```

To assign an administrator to an ADOM:

Enter the following CLI command:

```
config system admin user
    edit <name>
        set adom <adom_name>
    next
end
```

where `<name>` is the administrator user name and `<adom_name>` is the ADOM name.

system

Use system commands to configure options related to the overall operation of the FortiAnalyzer unit.



FortiAnalyzer CLI commands and variables are case sensitive.

admin	dns	log-fetch	route6
alert-console	docker	log-forward	saml
alertemail	fips	log-forward-service	sniffer
alert-event	fortiview	mail	snmp
auto-delete	global	metadata	soc-fabric
backup all-settings	ha	ntp	sql
central-management	interface	password-policy	syslog
certificate	locallog	report	web-proxy
connector	log	route	



TCP port numbers cannot be used by multiple services at the same time with the same IP address. If a port is already in use, it cannot be assigned to another service. For example, HTTPS and HTTP cannot have the same port number.

admin

Use the following commands to configure admin related settings.

admin group

Use this command to add, edit, and delete admin user groups.

Syntax

```
config system admin group
edit <name>
set member <string>
end
```

Variable	Description
<name>	Enter the name of the group you are editing or enter a new name to create an entry (character limit = 63).
member <string>	Add group members.

admin ldap

Use this command to add, edit, and delete Lightweight Directory Access Protocol (LDAP) users.

Syntax

```
config system admin ldap
edit <server>
    set adom-access {all | specify}
    set adom-attr <string>
    set adom <adom-name>
    set attributes <filter>
    set ca-cert <string>
    set cnid <string>
    set connect-timeout <integer>
    set dn <string>
    set filter <string>
    set group <string>
    set memberof-attr <string>
    set password <passwd>
    set port <integer>
    set profile-attr <string>
    set secondary-server <string>
    set secure {disable | ldaps | starttls}
    set server <string>
    set tertiary-server <string>
    set type {anonymous | regular | simple}
    set username <string>
end
```

Variable	Description
adom-access {all specify}	Set all or specify the ADOM access type (default = all).
<server>	Enter the name of the LDAP server or enter a new name to create an entry (character limit = 63).
adom-attr <string>	The attribute used to retrieve ADOM.
adom <adom-name>	Set the ADOM name to link to the LDAP configuration.
attributes <filter>	Attributes used for group searching (for multi-attributes, a use comma as a separator). For example: <ul style="list-style-type: none"> member uniquemember member,uniquemember

Variable	Description
ca-cert <string>	CA certificate name. This variable appears only when <code>secure</code> is set to <code>ldaps</code> or <code>starttls</code> .
cnid <string>	Enter the common name identifier (character limit = 20, default = <code>cn</code>).
connect-timeout <integer>	Set the LDAP connection timeout, in milliseconds (default = 500).
dn <string>	Enter the distinguished name.
filter <string>	Enter content for group searching. For example: (&(objectcategory=group)(member=*)) (&(objectclass=groupofnames)(member=*)) (&(objectclass=groupofuniquenames)(uniquemember=*)) (&(objectclass=posixgroup)(memberuid=*))
group <string>	Enter an authorization group. The authentication user must be a member of this group (full DN) on the server.
memberof-attr <string>	The attribute used to retrieve memeberof.
password <passwd>	Enter a password for the username above. This variable appears only when <code>type</code> is set to <code>regular</code> .
port <integer>	Enter the port number for LDAP server communication (1 - 65535, default = 389).
profile-attr <string>	The attribute used to retrieve admin profile.
secondary-server <string>	Enter the secondary LDAP server domain name or IPv4 address. Enter a new name to create a new entry.
secure {disable ldaps starttls}	Set the SSL connection type: <ul style="list-style-type: none"> <code>disable</code>: no SSL (default). <code>ldaps</code>: use LDAPS <code>starttls</code>: use STARTTLS
server <string>	Enter the LDAP server domain name or IPv4 address. Enter a new name to create a new entry.
tertiary-server <string>	Enter the tertiary LDAP server domain name or IPv4 address. Enter a new name to create a new entry.
type {anonymous regular simple}	Set a binding type: <ul style="list-style-type: none"> <code>anonymous</code>: Bind using anonymous user search <code>regular</code>: Bind using username/password and then search <code>simple</code>: Simple password authentication without search (default)
username <string>	Enter a username. This variable appears only when <code>type</code> is set to <code>regular</code> .

Example

This example shows how to add the LDAP user `user1` at the IPv4 address `206.205.204.203`.

```
config system admin ldap
edit user1
set server 206.205.204.203
set dn techdoc
```

```
set type regular
set username auth1
set password auth1_pwd
set group techdoc
end
```

admin profile

Use this command to configure access profiles. In a newly-created access profile, no access is enabled. Setting an option to `none` hides it from administrators with that profile assigned.

Syntax

```
config system admin profile
edit <profile_name>
    set adom-lock {none | read | read-write}
    set adom-switch {none | read | read-write}
    set allow-to-install {enable | disable}
    set change-password {enable | disable}
    set datamask {enable | disable}
    set datamask-custom-priority {enable | disable}
    set datamask-fields <fields>
    set datamask-key <passwd>
    set datamask-unmasked-time <integer>
    set description <text>
    set device-ap {none | read | read-write}
    set device-forticlient {none | read | read-write}
    set device-fortitxtender {none | read | read-write}
    set device-fortiswitch {none | read | read-write}
    set device-manager {none | read | read-write}
    set device-op {none | read | read-write}
    set device-policy-package-lock {none | read | read-write}
    set device-wan-link-load-balance {none | read | read-write}
    set event-management {none | read | read-write}
    set execute-playbook {none | read | read-write}
    set extension-access {none | read | read-write}
    set fabric-viewer {none | read | read-write}
    set fortirecorder-setting {none | read | read-write}
    set ipv6_trusthost1 <IPv6 prefix>
    set ipv6_trusthost2 <IPv6 prefix>
    set ipv6_trusthost3 <IPv6 prefix>
    .
    .
    .
    set ipv6_trusthost10 <IPv6 prefix>
    set log-viewer {none | read | read-write}
    set realtime-monitor {none | read | read-write}
    set report-viewer {none | read | read-write}
    set rpc-permit {none | read | read-write}
    set run-report {none | read | read-write}
    set scope {adom | global}
    set script-access {none | read | read-write}
    set super-user-profile {enable | disable}
    set system-setting {none | read | read-write}
```

```

set triage-events {none | read | read-write}
set trusthost1 <ip&netmask>
set trusthost2 <ip&netmask>
set trusthost3 <ip&netmask>
.
.
.
set trusthost10 <ip&netmask>
set update-incidents {none | read | read-write}
config datamask-custom-fields
    edit <field>
        set field-category {alert | all | fortiview | log | euba}
        set field-status {enable | disable}
        set field-type {email | ip | mac | string}
    next
end

```

Variable	Description
<profile>	Edit the access profile. Enter a new name to create a new profile (character limit = 35). The pre-defined access profiles are <i>Super_User</i> , <i>Standard_User</i> , and <i>Restricted_User</i> .
adom-lock {none read read-write}	Configure ADOM locking permissions for profile: <ul style="list-style-type: none"> • none: No permission (default). • read: Read permission. • read-write: Read-write permission. Controlled functions: ADOM locking. Dependencies: type must be system
adom-switch {none read read-write}	Configure administrative domain (ADOM) permissions for this profile. Controlled functions: ADOM settings in DVM, ADOM settings in All ADOMs page (under System Settings tab) Dependencies: If system-setting is none, the All ADOMs page is not accessible.
allow-to-install {enable disable}	Enable/disable allowing restricting users to install objects to the devices (default = enable).
change-password {enable disable}	Enable/disable allowing restricted users to change their password (default = disable).
datamask {enable disable}	Enable/disable data masking (default = disable).
datamask-custom-priority {enable disable}	Enable/disable custom field search priority.
datamask-fields <fields>	Enter that data masking fields, separated by spaces. <ul style="list-style-type: none"> • dstip: Destination IP • dstname: Destination name • email: Email • message: Message • srcip: Source IP • srcmac: Source MAC

Variable	Description
	<ul style="list-style-type: none"> <i>srcname</i>: Source name <i>user</i>: User name
datamask-key <passwd>	Enter the data masking encryption key.
datamask-unmasked-time <integer>	Enter the time without data masking, in days (default = 0).
description <string>	Enter a description for this access profile (character limit = 1023). Enclose the description in quotes if it contains spaces.
device-ap {none read read-write}	Set the AP Manager permissions (default = none).
device-forticlient {none read read-write}	Set the FortiClient Manager permissions (default = none).
device-fortiextender {none read read-write}	Set the FortiExtender Manager permissions (default = none).
device-fortiswitch {none read read-write}	Set the FortiSwitch Manager permissions (default = none).
device-manager {none read read-write}	<p>Enter the level of access to Device Manager settings for this profile (default = none).</p> <p>This command corresponds to the Device Manager option in the GUI administrator profile.</p> <p>Controlled functions: Device Manager</p>
device-op {none read read-write}	<p>Add the capability to add, delete, and edit devices to this profile (default = none).</p> <p>This command corresponds to the Add/Delete Devices/Groups option in the GUI administrator profile. This is a sub-setting of <i>device-manager</i>.</p> <p>Controlled functions: Add or delete devices or groups</p>
device-policy-package-lock {none read read-write}	<p>Configure device policy package locking permissions for this profile (default = none).</p> <p>Controlled functions: Policy package locking.</p> <p>Dependencies: <i>type</i> must be <i>system</i></p>
device-wan-link-load-balance {none read read-write}	Set the SD-WAN permissions (default = none).
event-management {none read read-write}	<p>Set the Event Management permissions (default = none).</p> <p>This command corresponds to the Event Management option in the GUI administrator profile.</p> <p>Controlled functions: Event Management tab and all its operations</p>
execute-playbook {none read read-write}	<p>Configure execute playbook permissions:</p> <ul style="list-style-type: none"> <i>none</i>: No permission (default). <i>read</i>: Read permission. <i>read-write</i>: Read-write permission.

Variable	Description
extension-access {none read read-write}	Manage extension access (default = none).
fabric-viewer {none read read-write}	Configure Fabric Viewer permissions: <ul style="list-style-type: none"> • none: No permission (default). • read: Read permission. • read-write: Read-write permission.
fortirecorder-setting {none read read-write}	Set the FortiRecorder permissions (default = none). This command corresponds to the FortiRecorder option in the GUI administrator profile. Controlled functions: FortiRecorder tab and all its operations Note: This command is only functional on hardware FortiAnalyzer devices.
ipv6_trusthost1 <IPv6 prefix> ipv6_trusthost2 <IPv6 prefix> ipv6_trusthost3 <IPv6 prefix> ... ipv6_trusthost10 <IPv6 prefix>	The admin user trusted host IPv6 address. Defaults = ipv6_trusthost1: ::/0 for all others: ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128 for none
log-viewer {none read read-write}	Set the Log View permissions (default = none). This command corresponds to the Log View option in the GUI administrator profile. Controlled functions: Log View and all its operations
realtime-monitor {none read read-write}	Enter the level of access to the Drill Down configuration settings for this profile (default = none).
report-viewer {none read read-write}	Set the Reports permissions (default = none). This command corresponds to the Reports option in the GUI administrator profile. Controlled functions: Reports tab and all its operations
rpc-permit {none read read-write}	Set the rpc-permission (default = none): <ul style="list-style-type: none"> • none: No permission. • read: Read permission. • read-write: Read-write permission.
run-report {none read read-write}	Configure run reports permission for this profile: <ul style="list-style-type: none"> • none: No permission (default). • read: Read permission. • read-write: Read-write permission.
scope (Not Applicable)	CLI command is not in use.
script-access {none read read-write}	Configure script access (default = none).

Variable	Description
super-user-profile {enable disable}	Enable/disable the super user profile (default = disable).
system-setting {none read read-write}	Configure System Settings permissions for this profile (default = none). This command corresponds to the System Settings option in the GUI administrator profile. Controlled functions: System Settings tab, All the settings under System setting
triage-events {none read read-write}	Set the triage events permissions for this profile (default = none).
trusthost1 <ip&netmask> trusthost2 <ip&netmask> trusthost2 <ip&netmask> ... trusthost10 <ip&netmask>	The admin user trusted host IP address. Defaults : trusthost1: 0.0.0.0.0.0.0.0 for all others: 255.255.255.255.255.255.255.255 for none
update-incidents {none read read-write}	Create/update incidents (default = none).
Variables for config datamask-custom-fields subcommand:	
<field>	Enter the custom field name.
field-category {alert all fortiview log euba}	Enter the field category (default = all).
field-status {enable disable}	Enable/disable the field (default = enable).
field-type {email ip mac string}	Enter the field type (default = string).

admin radius

Use this command to add, edit, and delete administration RADIUS servers.

Syntax

```

config system admin radius
edit <server>
    set auth-type {any | chap | mschap2 | pap}
    set nas-ip <ipv4_address>
    set port <integer>
    set secondary-secret <passwd>
    set secondary-server <string>
    set secret <passwd>
    set server <string>
end

```

Variable	Description
<server>	Enter the name of the RADIUS server or enter a new name to create an entry (character limit = 63).
auth-type {any chap mschap2 pap}	The authentication protocol the RADIUS server will use. <ul style="list-style-type: none"> any: Use any supported authentication protocol (default). mschap2: Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2). chap: Challenge Handshake Authentication Protocol (CHAP). pap: Password Authentication Protocol (PAP).
nas-ip <ipv4_address>	The network access server (NAS) IPv4 address and called station ID.
port <integer>	The RADIUS server port number (1 - 65535, default = 1812).
secondary-secret <passwd>	The password to access the RADIUS secondary-server (character limit = 64).
secondary-server <string>	The RADIUS secondary-server DNS resolvable domain name or IPv4 address.
secret <passwd>	The password to access the RADIUS server (character limit = 64).
server <string>	The RADIUS server DNS resolvable domain name or IPv4 address.

Example

This example shows how to add the RADIUS server `RAID1` at the IPv4 address `206.205.204.203` and set the shared secret as `R1a2D3i4U5s`.

```
config system admin radius
  edit RAID1
    set server 206.205.204.203
    set secret R1a2D3i4U5s
  end
```

admin setting

Use this command to configure system administration settings, including web administration ports, timeout, and language.

Syntax


```
config system admin setting
  set access-banner {enable | disable}
  set admin-https-redirect {enable | disable}
  set admin-login-max <integer>
  set admin_server_cert <admin_server_certificate>
  set auth-addr <string>
  set auth-port <integer>
  set banner-message <string>
  set fsw-ignore-platform-check {enable | disable}
  set gui-theme <theme>
  set http_port <integer>
```

```

set https_port <integer>
set idle_timeout <integer>
set idle_timeout_api <integer>
set idle_timeout_gui <integer>
set idle_timeout_sso <integer>
set objects-force-deletion {enable | disable}
set preferred-fgfm-intf <string>
set shell-access {enable | disable}
set shell-password <passwd>
set show-add-multiple {enable | disable}
set show-checkbox-in-table {enable | disable}
set show-device-import-export {enable | disable}
set show-fct-manager {enable | disable}
set show_hostname {enable | disable}
set show-log-forwarding {enable | disable}
set unreg_dev_opt {add_allow_service | add_no_service}
set webadmin_language {auto_detect | english | french | japanese | korean |
    simplified_chinese | spanish | traditional_chinese}
end

```

Variable	Description
access-banner {enable disable}	Enable/disable the access banner (default= disable).
admin-https-redirect {enable disable}	Enable/disable redirection of HTTP admin traffic to HTTPS (default= enable).
admin-login-max <integer>	Set the maximum number of admin users that be logged in at one time (1 - 256, default = 256).
admin_server_cert <admin_server_certificate>	Enter the name of an https server certificate to use for secure connections (default = server.crt). FortiAnalyzer has server.crt and Fortinet_Local certificates pre-loaded.
auth-addr <string>	Enter the IP which is used by FortiGate to authorize FortiAnalyzer.
auth-port <integer>	Set the port which is used by FortiGate to authorize FortiAnalyzer (default = 443).
banner-message <string>	Set the banner messages (character limit = 32768).
fsw-ignore-platform-check {enable disable}	Enable/disable FortiSwitch Manager switch platform support check (default = disable).
gui-theme <theme>	Configure the GUI theme (default = blue).
http_port <integer>	Enter the HTTP port number for web administration (1 - 65535, default = 80).
https_port <integer>	Enter the HTTPS port number for web administration (1 - 65535, default = 443).
idle_timeout <integer>	Enter the idle timeout value, in seconds (60 - 28800, default = 900). The <code>idle_timeout_api</code> , <code>idle_timeout_gui</code> , and <code>idle_timeout_sso</code> settings control the idle timeout for API, GUI, and SSO. The <code>idle_timeout</code> setting controls all other idle timeout, including idle timeout for SSH and console.
idle_timeout_api <integer>	Enter the idle timeout for the API sessions, in seconds (1 - 28800, default = 900).
idle_timeout_gui <integer>	Enter the idle timeout for the GUI sessions, in seconds (60 - 28800, default = 900).

Variable	Description
idle_timeout_sso <integer>	Enter the idle timeout for the SSO sessions, in seconds (60 - 28800, default = 900).
objects-force-deletion {enable disable}	Enable/disable forced deletion of used objects (default = enable).
preferred-fgfm-intf <string>	Preferred interface for FGFM connection.
shell-access {enable disable}	Enable/disable shell access (default = disable).
shell-password <passwd>	Enter the password to use for shell access.
show-add-multiple {enable disable}	Enable/disable show the add multiple button in the GUI (default = disable).
show-checkbox-in-table {enable disable}	Enable/disable show checkboxes in tables in the GUI (default = disable).
show-device-import-export {enable disable}	Enable/disable import/export of ADOM, device, and group lists (default = disable).
show-fct-manager {enable disable}	<div> <div>  </div> <div> <p>Although still available in FortiAnalyzer 7.0, this command has no impact on the GUI.</p> <p>This is because the FortiClient module is a FortiManager feature, which are not available in FortiAnalyzer 6.2 and up.</p> </div> </div>
show_hostname {enable disable}	Enable/disable showing the hostname on the GUI login page (default = disable).
show-log-forwarding {enable disable}	Enable/disable show log forwarding tab in analyzer mode (default= enable).
unreg_dev_opt {add_allow_service add_no_service}	Select action to take when an unregistered device connects to FortiAnalyzer: <ul style="list-style-type: none"> • <code>add_allow_service</code>: Add unregistered devices and allow service requests (default). • <code>add_no_service</code>: Add unregistered devices and deny service requests.
webadmin_language {auto_detect english french japanese korean simplified_chinese spanish traditional_chinese}	Enter the language to be used for web administration. The following options are available: <ul style="list-style-type: none"> • <code>auto_detect</code>: Automatically detect language (default) • <code>english</code>: English • <code>french</code>: French • <code>japanese</code>: Japanese • <code>korean</code>: Korean • <code>simplified_chinese</code>: Simplified Chinese • <code>spanish</code>: Spanish • <code>traditional_chinese</code>: Traditional Chinese

Use the show command to display the current configuration if it has been changed from its default value:

```
show system admin setting
```

admin tacacs

Use this command to add, edit, and delete administration TACACS+ servers.

Syntax

```
config system admin tacacs
  edit <server>
    set authen-type {ascii | auto | chap | mschap | pap}
    set authorization {enable | disable}
    set key <passwd>
    set port <integer>
    set secondary-key <passwd>
    set secondary-server <string>
    set server <string>
    set tertiary-key <passwd>
    set tertiary-server <string>
end
```

Variable	Description
<server>	Enter the name of the TACACS+ server or enter a new name to create an entry (character limit = 63).
authen-type {ascii auto chap mschap pap}	Choose which authentication type to use: <ul style="list-style-type: none"> • ascii: ASCII • auto: Uses PAP, MSCHAP, and CHAP (in that order) (default). • chap: Challenge Handshake Authentication Protocol (CHAP) • mschap: Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) • pap: Password Authentication Protocol (PAP).
authorization {enable disable}	Enable/disable TACACS+ authorization (default = disable).
key <passwd>	Key to access the server (character limit = 128).
port <integer>	Port number of the TACACS+ server (1 - 65535, default = 49).
secondary-key <passwd>	Key to access the secondary server (character limit = 128).
secondary-server <string>	Secondary server domain name or IPv4 address.
server <string>	The server domain name or IPv4 address.
tertiary-key <passwd>	Key to access the tertiary server (character limit = 128).
tertiary-server <string>	Tertiary server domain name or IPv4 address.

Example

This example shows how to add the TACACS+ server `TAC1` at the IPv4 address `206.205.204.203` and set the key as `R1a2D3i4U5s`.

```
config system admin tacacs
  edit TAC1
```

```
set server 206.205.204.203
set key R1a2D3i4U5s
end
```

admin user

Use this command to add, edit, and delete administrator accounts.

Use the admin account or an account with System Settings read and write privileges to add new administrator accounts and control their permission levels. Each administrator account must include a minimum of an access profile. The access profile list is ordered alphabetically, capitals first. If custom profiles are defined, it may change the default profile from Restricted_User. You cannot delete the admin administrator account. You cannot delete an administrator account if that user is logged on.



You can create meta-data fields for administrator accounts. These objects must be created using the FortiAnalyzer GUI. The only information you can add to the object is the value of the field (pre-determined text/numbers). For more information, see *System Settings* in the *FortiAnalyzer Administration Guide*.

Syntax

```
config system admin user
edit <name_str>
    set adom-access {all | exclude | specify}
    set login-max <integer>
    set password <passwd>
    set change-password {enable | disable}
    set th-from-profile <integer>
    set th6-from-profile <integer>
    set trusthost1 <ipv4_mask>
    set trusthost2 <ipv4_mask>
    set trusthost3 <ipv4_mask>
    ...
    set trusthost10 <ipv4_mask>
    set ipv6_trusthost1 <ipv6_mask>
    set ipv6_trusthost2 <ipv6_mask>
    set ipv6_trusthost3 <ipv6_mask>
    ...
    set ipv6_trusthost10 <ipv6_mask>
    set profileid <profile-name>
    set adom <adom_name(s)>
    set dev-group <group-name>
    set policy-package <policy-package-name>
    set description <string>
    set user_type {group | ldap | local | pki-auth | radius | tacacs-plus}
    set group <string>
    set ldap-server <string>
    set radius_server <string>
    set tacacs-plus-server <string>
    set ssh-public-key1 <key-type> <key-value>
    set ssh-public-key2 <key-type>, <key-value>
    set ssh-public-key3 <key-type> <key-value>
    set avatar <string>
```

```
set wildcard <enable | disable>
set ext-auth-accprofile-override <enable | disable>
set ext-auth-adom-override <enable | disable>
set ext-auth-group-match <string>
set password-expire <yyyy-mm-dd>
set force-password-change {enable | disable}
set fingerprint <string>
set subject <string>
set ca <string>
set two-factor-auth {enable | disable}
set rpc-permit {none | read-only | read-write}
set use-global-theme {enable | disable}
set user-theme {astronomy | autumn | binary-tunnel | blue | calla-lily | canyon |
    cave | contrast-dark | diving | dreamy | fish | green | landscape | melongene
    | mountain | northern-light | parrot | penguin | polar-bear | red | space |
    spring | summer | technology | twilight | winter | zebra}
set last-name <string>
set first-name <string>
set email-address <string>
set phone-number <string>
set mobile-number <string>
set pager-number <string>
config meta-data
    edit <fieldname>
        set fieldlength
        set fieldvalue <string>
        set importance
        set status
    end
config dashboard-tabs
    edit tabid <integer>
        set name <string>
    end
config dashboard
    edit moduleid
        set name <string>
        set column <column_pos>
        set diskio-content-type
        set diskio-period {1hour | 24hour | 8hour}
        set refresh-interval <integer>
        set status {close | open}
        set tabid <integer>
        set widget-type <string>
        set log-rate-type {device | log}
        set log-rate-topn {1 | 2 | 3 | 4 | 5}
        set log-rate-period {1hour | 2min | 6hours}
        set res-view-type {history | real-time}
        set res-period {10min | day | hour}
        set res-cpu-display {average | each}
        set num-entries <integer>
        set time-period {1hour | 24hour | 8hour}
    end
end
```


Variable	Description
<name_string>	Enter the name of the admin user or enter a new name to create a new user (character limit = 35).
adom-access {all exclude specify}	Set all/specify/exclude ADOM access mode (default = specify).
login-max <integer>	Set the maximum number of login sessions for this user (default = 32).
password <passwd>	Enter a password for the administrator account (character limit = 128). For improved security, the password should be at least 6 characters long. This variable is available only if <code>user_type</code> is <code>local</code> .
change-password {enable disable}	Enable/disable allowing restricted users to change their password (default = disable).
th-from-profile <integer>	
th6-from-profile <integer>	
trusthost1 <ipv4_mask> trusthost2 <ipv4_mask> ... trusthost10 <ipv4_mask>	Optionally, type the trusted host IPv4 address and network mask from which the administrator can log in to the FortiAnalyzer system. You can specify up to ten trusted hosts. Setting trusted hosts for all of your administrators can enhance the security of your system. Defaults: <code>trusthost1: 0.0.0.0 0.0.0.0 for all</code> <code>others: 255.255.255.255 255.255.255.255 for none</code>
ipv6_trusthost1 <ipv6_mask> ipv6_trusthost2 <ipv6_mask> ... ipv6_trusthost10 <ipv6_mask>	Optionally, type the trusted host IPv6 address from which the administrator can log in to the FortiAnalyzer system. You can specify up to ten trusted hosts. Setting trusted hosts for all of your administrators can enhance the security of your system. Defaults: <code>ipv6_trusthost1: ::/0 for all</code> <code>others: ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128 for none</code>
profileid <profile-name>	Enter the name of the access profile to assign to this administrator account (character limit = 35, default = <code>Restricted_User</code>). Access profiles control administrator access to FortiAnalyzer features.
adom <adom_name(s)>	Enter the name(s) of the ADOM(s) the administrator belongs to. Any configuration of ADOMs takes place via the FortiAnalyzer GUI.
dev-group <group-name>	Enter the device group that the admin use can access. This option can only be used for administrators with access to only one ADOM.
policy-package {<adom name>: <policy package id> <adom policy folder name>/ <package name> all_policy_packages}	Policy package access

Variable	Description
description <string>	Enter a description for this administrator account (character limit = 127). Enclose the description in quotes if it contains spaces.
user_type {group ldap local pki-auth radius tacacs-plus}	Select the administrator type: <ul style="list-style-type: none"> • group: The administrator is a member of a administrator group. • ldap: An LDAP server verifies the administrator's password. • local: The FortiAnalyzer system verifies the administrator's password (default). • pki-auth: The administrator uses PKI. • radius: A RADIUS server verifies the administrator's password. • tacacs-plus: A TACACS+ server verifies the administrator's password.
group <string>	Enter the group name.
ldap-server <string>	Enter the LDAP server name if the user type is set to LDAP.
radius_server <string>	Enter the RADIUS server name if the user type is set to RADIUS.
tacacs-plus-server <string>	Enter the TACACS+ server name if the user type is set to TACACS+.
ssh-public-key1 <key-type> <key-value>	You can specify the public keys of up to three SSH clients. These clients are authenticated without being asked for the administrator password. You must create the public-private key pair in the SSH client application. <key type> is ssh-dss for a DSA key, ssh-rsa for an RSA key. <key-value> is the public key string of the SSH client.
ssh-public-key2 <key-type> <key-value>	
ssh-public-key3 <key-type> <key-value>	
avatar <string>	Image file for the administrator's avatar (maximum 4K base64 encode).
wildcard <enable disable>	Enable/disable wildcard remote authentication (default = disable).
ext-auth-accprofile-override <enable disable>	Enable/disable allowing the use of the access profile provided by the remote authentication server (default = disable).
ext-auth-adom-override <enable disable>	Enable/disable allowing the use of the ADOM provided by the remote authentication server (default = disable). In order to support vendor specific attributes (VSA), the authentication server requires a dictionary to define which VSAs to support. The Fortinet RADIUS vendor ID is 12365. The <code>Fortinet-Vdom-Name</code> attribute is used by this command.
ext-auth-group-match <string>	Only admin users that belong to this group are allowed to log in.
password-expire <yyyy-mm-dd>	When enforcing the password policy, enter the date that the current password will expire.
force-password-change {enable disable}	Enable/disable force password change on next log in.
fingerprint <string>	PKI user certificate fingerprint based on MD5, SHA-1, or SHA-256 hash function. Format the fingerprint by removing spaces or replacing them with ':'. For example, 0123abcd... or 01:23:ab:cd....

Variable	Description
	This command is available when a PKI administrator account is configured.
subject <string>	PKI user certificate name constraints. This command is available when a PKI administrator account is configured.
ca <string>	PKI user certificate CA (CA name in local). This command is available when a PKI administrator account is configured.
two-factor-auth {enable disable}	Enable/disable two-factor authentication (certificate + password) (default = disable). This command is available when a PKI administrator account is configured.
rpc-permit {none read-only read-write}	Set the permission level for log in via Remote Procedure Call (RPC) (default = none).
use-global-theme {enable disable}	Enable/disable global theme for administration GUI (default = enable).
user-theme {astronomy autumn binary-tunnel blue calla-lily canyon cave contrast-dark diving dreamy fish green landscape melongene mountain northern-light parrot penguin polar-bear red space spring summer technology twilight winter zebra}	Set the color scheme to use for the admin user GUI (default = blue): astronomy: Astronomy autumn: Autumn binary-tunnel: Binary Tunnel blue: Blueberry calla-lily: Calla Lily canyon: Canyon cave: Cave contrast-dark: High Contrast Dark diving: Diving dreamy: Dreamy fish: Fish green: Kiwi landscape: Landscape melongene: Plum mountain: Mountain northern-light: Northern Light parrot: Parrot penguin: Penguin polar-bear: Polar Bear red: Cherry space: Space spring: Spring summer: Summer technology: Technology twilight: Twilight

Variable	Description
	winter: Winter zebra: Zebra This command is available when <code>use-global-theme</code> is disabled.
last-name <string>	Administrator's last name (character limit = 63).
first-name <string>	Administrator's first name (character limit = 63).
email-address <string>	Administrator's email address.
phone-number <string>	Administrator's phone number.
mobile-number <string>	Administrator's mobile phone number.
pager-number <string>	Administrator's pager number.
Variables for <code>config meta-data</code> subcommand: This subcommand can only change the value of an existing field. To create a new metadata field, use the <code>config system metadata</code> command.	
fieldname	The label/name of the field (read-only, default = 50). Enclose the name in quotes if it contains spaces.
fieldlength	The maximum number of characters allowed for this field (read-only, default = 50).
fieldvalue <string>	Enter a pre-determined value for the field. This is the only value that can be changed with the <code>config meta-data</code> subcommand (character limit = 255).
importance	Indicates whether the field is compulsory (<code>required</code>) or optional (<code>optional</code>) (read-only, default = <code>optional</code>).
status	The status of the field (read-only, default = <code>enable</code>).
Variables for <code>config dashboard-tabs</code> subcommand:	
tabid <integer>	Tab ID.
name <string>	Tab name.
Variables for <code>config dashboard</code> subcommand:	
moduleid	Widget ID.
name <string>	Widget name (character limit = 63).
column <column_pos>	Widget column ID (default = 0).
diskio-content-type {blks iops util}	Set the Disk I/O Monitor widget's chart type. <ul style="list-style-type: none"> • <code>blks</code>: the amount of data of I/O requests. • <code>iops</code>: the number of I/O requests. • <code>util</code>: bandwidth utilization (default).
diskio-period {1hour 24hour 8hour}	Set the Disk I/O Monitor widget's data period (default = 1hour).

Variable	Description
refresh-interval <integer>	Widget refresh interval (default = 300).
status {close open}	Widget opened/closed status (default = open).
tabid <integer>	ID of the tab where the widget is displayed (default = 0).
widget-type <string>	Widget type: <ul style="list-style-type: none"> • alert: Alert Message Console • devsummary: Device Summary • disk-io: Disk I/O • jsconsole: CLI Console • licinfo: License Information • log-rcvd-fwd: Receive Rate v. Forwarding Rate • logdb-lag: Log Insert Lag Time • logdb-perf: Insert Rate vs Receive Rate • logrecv: Logs/Data Received (this widget has been deprecated) • raid: Disk Monitor • rpteng: Report Engine (this widget has been deprecated) • statistics: Statistics (this widget has been deprecated) • sysinfo: System Information • sysop: Unit Operation • sysres: System Resources • top-lograte: Log Receive Monitor
log-rate-type {device log}	Log receive monitor widget's statistics breakdown options (default = device).
log-rate-topn {1 2 3 4 5}	Log receive monitor widgets's number of top items to display (default = 5).
log-rate-period {1hour 2min 6hours}	Log receive monitor widget's data period (default = 2min).
res-view-type {history real-time}	Widget's data view type (default = history).
res-period {10min day hour}	Widget data period: <ul style="list-style-type: none"> • 10min: Last 10 minutes (default). • day: Last day. • hour: Last hour.
res-cpu-display {average each}	Widget CPU display type: <ul style="list-style-type: none"> • average: Average usage of CPU (default). • each: Each usage of CPU.
num-entries <integer>	Number of entries (default = 10).
time-period {1hour 24hour 8hour}	Set the Log Database Monitor widget's data period (default = 1hour).

Using trusted hosts

Setting trusted hosts for all of your administrators increases the security of your network by further restricting administrative access. In addition to knowing the password, an administrator must connect only through the subnet or

subnets you specify. You can even restrict an administrator to a single IPv4 address if you define only one trusted host IPv4 address with a netmask of 255.255.255.255.

When you set trusted hosts for all administrators, the FortiAnalyzer system does not respond to administrative access attempts from any other hosts. This provides the highest security. If you leave even one administrator unrestricted, the unit accepts administrative access attempts on any interface that has administrative access enabled, potentially exposing the unit to attempts to gain unauthorized access.

The trusted hosts you define apply both to the GUI and to the CLI when accessed through SSH. CLI access through the console connector is not affected.

Example

Use the following commands to add a new administrator account named `admin_2` with the password set to `p8ssw0rd` and the `Super_User` access profile. Administrators that log in to this account will have administrator access to the FortiAnalyzer system from any IPv4 address.

```
config system admin user
  edit admin_2
    set description "Backup administrator"
    set password p8ssw0rd
    set profileid Super_User
  end
```

alert-console

Use this command to configure the alert console options. The alert console appears on the dashboard in the GUI.

Syntax

```
config system alert-console
  set period {1 | 2 | 3 | 4 | 5 | 6 | 7}
  set severity-level {information | notify | warning | error | critical | alert |
    emergency}
end
```

Variable	Description
<code>period {1 2 3 4 5 6 7}</code>	Enter the number of days to keep the alert console alerts (default = 7).
<code>severity-level {information notify warning error critical alert emergency}</code>	Enter the minimum severity level to display on the alert console on the dashboard: <ul style="list-style-type: none"> <code>emergency</code>: The unit is unusable (default). <code>alert</code>: Immediate action is required. <code>critical</code>: Functionality is affected. <code>error</code>: Functionality is probably affected. <code>warning</code>: Functionality might be affected. <code>notification</code>: Information about normal events. <code>information</code>: General information about unit operations.

Example

This example sets the alert console message display to warning for a duration of three days.

```
config system alert-console
  set period 3
  set severity-level warning
end
```

alertemail

Use this command to configure alert email settings for your FortiAnalyzer unit.

All variables are required when authentication is enabled.

Syntax

```
config system alertemail
  set authentication {enable | disable}
  set fromaddress <email-address_string>
  set fromname <string>
  set smtppassword <passwd>
  set smtpport <integer>
  set smtpserver {<ipv4_address>|<fqdn_string>}
  set smtpuser <username>
end
```

Variable	Description
authentication {enable disable}	Enable/disable alert email authentication (default = enable).
fromaddress <email-address_string>	The email address the alert message is from. This is a required variable.
fromname <string>	The SMTP name associated with the email address. Enclose the name in quotes if it contains spaces.
smtppassword <passwd>	Set the SMTP server password (character limit = 39).
smtpport <integer>	The SMTP server port (1 - 65535, default = 25).
smtpserver {<ipv4_address> <fqdn_string>}	The SMTP server address, either a DNS resolvable host name or an IPv4 address.
smtpuser <username>	Set the SMTP server username (character limit= 63).

Example

Here is an example of configuring `alertemail`. Enable authentication, the alert is set in Mr. Customer's name and from his email address, the SMTP server port is the default port(25), and the SMTP server is at IPv4 address of 192.168.10.10.

```
config system alertemail
```

```

set authentication enable
set fromaddress customer@example.com
set fromname "Ms. Customer"
set smtpport 25
set smtpserver 192.168.10.10
end

```

alert-event

Use `alert-event` commands to configure the FortiAnalyzer unit to monitor logs for log messages with certain severity levels, or information within the logs. If the message appears in the logs, the FortiAnalyzer unit sends an email or SNMP trap to a predefined recipient(s) of the log message encountered. Alert event messages provide immediate notification of issues occurring on the FortiAnalyzer unit.

When configuring an alert email, you must configure at least one DNS server. The FortiGate unit uses the SMTP server name to connect to the mail server and must look up this name on your DNS server.



`alert-event` was removed from the GUI in FortiAnalyzer version 5.0.3. This command has been kept in the CLI for customers who previously configured this function.

Syntax

```

config system alert-event
edit <name_string>
    set enable-generic-text {enable | disable}
    set enable-severity-filter {enable | disable}
    set event-time-period {0.5 | 1 | 3 | 6 | 12 | 24 | 72 | 168}
    set generic-text <string>
    set num-events {1 | 5 | 10 | 50 | 100}
    set severity-filter {high | low | medium | medium-high | medium-low}
    set severity-level-comp {>= | = | <=}
    set severity-level-logs {no-check | information | notify | warning | error |
        critical | alert | emergency}
    config alert-destination
        edit destination_id <integer>
            set type {mail | snmp | syslog}
            set from <email_address>
            set to <email_address>
            set smtp-name <server_name>
            set snmp-name <server_name>
            set syslog-name <server_name>
        end
    end
end

```

Variable	Description
<name_string>	Enter a name for the alert event (character limit = 63).

Variable	Description
enable-generic-text {enable disable}	Enable generic text match (default = disable).
enable-severity-filter {enable disable}	Enable/disable alert severity filter (default = disable).
event-time-period {0.5 1 3 6 12 24 72 168}	The period of time in hours during which if the threshold number is exceeded, the event will be reported: <ul style="list-style-type: none"> 0.5: 30 minutes (default) 1: 1 hour 3: 3 hours 6: 6 hours 12: 12 hours 24: 1 day 72: 3 days 168: 1 week
generic-text <string>	Text that must be contained in a log to trigger alert (character limit = 255).
num-events {1 5 10 50 100}	Set the minimum number of events that must occur in the given interval before it is reported (default = 1).
severity-filter {high low medium medium-high medium-low}	Set the required log severity to trigger an alert (default = high).
severity-level-comp {>= = <=}	Set the log severity threshold comparison criterion (default = =). Log messages are monitored based on the log level. For example, alerts may be monitored if the messages are greater than or equal to (>=) the Warning log level.
severity-level-logs {no-check information notify warning error critical alert emergency}	Set the log severity threshold level. That is, the log level the FortiManager looks for when monitoring for alert messages. <ul style="list-style-type: none"> no-check: Do not check severity level for this log type (default). emergency: The unit is unusable. alert: Immediate action is required. critical: Functionality is affected. error: Functionality is probably affected. warning: Functionality might be affected. notification: Information about normal events. information: General information about unit operations.
Variables for <code>config alert-destination</code> subcommand:	
destination_id <integer>	Enter the table sequence number, beginning at 1.
type {mail snmp syslog}	Select the alert event message method of delivery: <ul style="list-style-type: none"> mail: Send email alert (default). snmp: Send SNMP trap. syslog: Send syslog message.

Variable	Description
from <email_address>	Enter the sender email address to use in alert emails. This is available when <code>type</code> is set to <code>mail</code> .
to <email_address>	Enter the recipient email address to use in alert emails. This is available when <code>type</code> is set to <code>mail</code> .
smtp-name <server_name>	Enter the name of the mail server. This is available when <code>type</code> is set to <code>mail</code> .
snmp-name <server_name>	Enter the snmp server name. This is available when <code>type</code> is set to <code>snmp</code> .
syslog-name <server_name>	Enter the syslog server name or IPv4 address. This is available when <code>type</code> is set to <code>syslog</code> .

Example

In the following example, the alert message is set to send an email to the administrator when 5 warning log messages appear over the span of three hours.

```
config system alert-event
  edit warning
    config alert-destination
      edit 1
        set type mail
        set from fmgr@example.com
        set to admin@example.com
        set smtp-name mail.example.com
      end
      set enable-severity-filter enable
      set event-time-period 3
      set severity-level-log warning
      set severity-level-comp =
      set severity-filter medium
    end
  end
```

auto-delete

Use this command to automatically delete policies for logs, reports, and archived and quarantined files.

Syntax

```
config system auto-delete
  config dlp-files-auto-deletion
    set retention {days | weeks | months}
    set runat <integer>
    set status {enable | disable}
    set value <integer>
  end
  config quarantine-files-auto-deletion
    set retention {days | weeks | months}
    set runat <integer>
```

```

        set status {enable | disable}
        set value <integer>
    end
    config log-auto-deletion
        set retention {days | weeks | months}
        set runat <integer>
        set status {enable | disable}
        set value <integer>
    end
    config report-auto-deletion
        set retention {days | weeks | months}
        set runat <integer>
        set status {enable | disable}
        set value <integer>
    end
end
end

```

Variable	Description
dlp-files-auto-deletion	Automatic deletion policy for DLP archives.
quarantine-files-auto-deletion	Automatic deletion policy for quarantined files.
log-auto-deletion	Automatic deletion policy for device logs.
report-auto-deletion	Automatic deletion policy for reports.
retention {days weeks months}	Automatic deletion in days, weeks, or months (default = days).
runat <integer>	Automatic deletion run at (0 - 23) o'clock (default = 0).
status {enable disable}	Enable/disable automatic deletion (default = disable).
value <integer>	Automatic deletion in x days, weeks, or months (default = 0).

backup all-settings

Use this command to set or check the settings for scheduled backups.

An MD5 checksum is automatically generated in the event log when backing up the configuration. You can verify a backup by comparing the checksum in the log entry with that of the backup file.

Syntax

```

config system backup all-settings
    set status {enable | disable}
    set server {<ipv4_address>|<fqdn_str>}
    set user <username>
    set directory <string>
    set week_days {monday tuesday wednesday thursday friday saturday sunday}
    set time <hh:mm:ss>
    set protocol {ftp | scp | sftp}
    set passwd <passwd>
    set cert <certificate_name>

```

```

    set crptpasswd <passwd>
end

```

Variable	Description
status {enable disable}	Enable/disable scheduled backups (default = disable).
server {<ipv4_address> <fqdn_str>}	Enter the IPv4 address or DNS resolvable host name of the backup server.
user <username>	Enter the user account name for the backup server (character limit = 63).
directory <string>	Enter the name of the directory on the backup server in which to save the backup file.
week_days {monday tuesday wednesday thursday friday saturday sunday}	Enter the days of the week on which to perform backups. You may enter multiple days.
time <hh:mm:ss>	Enter the time of day to perform the backup. Time is required in the form <hh:mm:ss>.
protocol {ftp scp sftp}	Enter the transfer protocol (default = sftp).
passwd <passwd>	Enter the password for the backup server (character limit = 127).
cert <certificate_name>	SSH certificate for authentication. Only available if the protocol is set to scp. The SSH certificate object must already be configured. See certificate ssh on page 72 .
crptpasswd <passwd>	Optional password to protect backup content (character limit = 63).

Example

This example shows a whack where backup server is 172.20.120.11 using the admin account with no password, saving to the /usr/local/backup directory. Backups are done on Mondays at 1:00pm using ftp.

```

config system backup all-settings
    set status enable
    set server 172.20.120.11
    set user admin
    set directory /usr/local/backup
    set week_days monday
    set time 13:00:00
    set protocol ftp
end

```

central-management

Use this command to set or check the settings for central management.

Syntax

```
config system central-management
  set type {fortimanager}
  set allow-monitor {enable | disable}
  set authorized-manager-only {enable | disable}
  set fmg <string>
  set enc-algorithm {default | high | low}
  set mgmtid <integer>
  set serial-number <serial_number_string>
end
```

Variable	Description
type {fortimanager}	Type of management server (default = fortimanager).
allow-monitor {enable disable}	Enable/disable remote monitoring of the device (default = enable).
authorized-manager-only {enable disable}	Enable/disable restricted to authorize manager only setting (default = enable).
fmg <string>	Set the IP address or FQDN of the FortiManager (character limit = 31).
enc-algorithm {default high low}	Set the SSL communication encryption algorithms: <ul style="list-style-type: none"> default: SSL communication with high and medium encryption algorithms (default) high: SSL communication with high encryption algorithms low: SSL communication with low encryption algorithms
mgmtid <integer>	
serial-number <serial_number_string>	Set the device serial number. You can enter up to 5 serial numbers.

Use the show command to display the current configuration if it has been changed from its default value:

```
show system central-management
```

certificate

Use the following commands to configure certificate related settings.

certificate ca

Use this command to install Certificate Authority (CA) root certificates.

When a CA processes your Certificate Signing Request (CSR), it sends you the CA certificate, the signed local certificate and the Certificate Revocation List (CRL).

The process for obtaining and installing certificates is as follows:

1. Use the `execute certificate local generate` command to generate a CSR.
2. Send the CSR to a CA. The CA sends you the CA certificate, the signed local certificate and the CRL.
3. Use the `system certificate local` command to install the signed local certificate.
4. Use the `system certificate ca` command to install the CA certificate. Depending on your terminal software, you can copy the certificate and paste it into the command.

Syntax

```
config system certificate ca
  edit <ca_name>
    set ca <certificate>
    set comment <string>
  end
```

Variable	Description
<ca_name>	Enter a name for the CA certificate (character limit = 35).
ca <certificate>	Enter or retrieve the CA certificate in PEM format.
comment <string>	Optionally, enter a descriptive comment (character limit = 127).

certificate crl

Use this command to configure CRLs.

Syntax

```
config system certificate crl
  edit <name>
    set crl <crl>
    set comment <string>
    set http-url <string>
    set update-interval <integer>
  end
```

Variable	Description
<name>	Enter a name for the CRL (character limit = 35).
crl <crl>	Enter or retrieve the CRL in PEM format.
comment <string>	Optionally, enter a descriptive comment for this CRL (character limit = 127).
http-url <string>	Set the HTTP server URL for CRL auto-update.
update-interval <integer>	Set the CRL auto-update interval, in minutes (minimum = 3, default = 1440).

certificate local

Use this command to install local certificates. When a CA processes your CSR, it sends you the CA certificate, the signed local certificate and the CRL.

The process for obtaining and installing certificates is as follows:

1. Use the `execute certificate local generate` command to generate a CSR.
2. Send the CSR to a CA. The CA sends you the CA certificate, the signed local certificate and the CRL.
3. Use the `system certificate local` command to install the signed local certificate.
4. Use the `system certificate ca` command to install the CA certificate. Depending on your terminal software, you can copy the certificate and paste it into the command.

Syntax

```
config system certificate local
  edit <cert_name>
    set password <passwd>
    set comment <string>
    set certificate <certificate_PEM>
    set private-key <prkey>
    set csr <csr_PEM>
  next
end
```

Variable	Description
<cert_name>	Enter the local certificate name (character limit = 35).
password <passwd>	Enter the local certificate password (character limit = 67).
comment <string>	Enter any relevant information about the certificate (character limit = 127).
certificate <certificate_PEM>	Enter the signed local certificate in PEM format.
You should not modify the following variables if you generated the CSR on this unit.	
private-key <prkey>	The private key in PEM format.
csr <csr_PEM>	The CSR in PEM format.

certificate oftp

Use this command to install OFTP certificates and keys.

Syntax

```
config system certificate oftp
  set certificate <certificate>
  set comment <string>
  set local {Fortinet_Local | Fortinet_Local2}
  set mode {custom | default | local}
```

```

    set password <passwd>
    set private-key <key>
end

```

Variable	Description
certificate <certificate>	PEM format certificate.
comment <string>	OFTP certificate comment (character limit = 127).
local {Fortinet_Local Fortinet_Local2}	Choose from the two available local certificates.
mode {custom default local}	Mode of certificates used by OFTPD (default = default): <ul style="list-style-type: none"> • custom: Use a custom certificate. • default: Default mode. • local: Use a local certificate.
password <passwd>	Password for encrypted 'private-key', unset for non-encrypted.
private-key <key>	PEM format private key.

certificate remote

Use this command to install remote certificates

Syntax

```

config system certificate remote
edit <cert_name>
    set cert <certificate>
    set comment <string>
next
end

```

Variable	Description
<cert_name>	Enter the remote certificate name (character limit = 35).
cert <certificate>	The remote certificate.
comment <string>	Optionally, enter a descriptive comment (character limit = 127).

certificate ssh

Use this command to install SSH certificates and keys.

The process for obtaining and installing certificates is as follows:

1. Use the `execute certificate local generate` command to generate a CSR.
2. Send the CSR to a CA. The CA sends you the CA certificate, the signed local certificate and the CRL.
3. Use the `system certificate local` command to install the signed local certificate.

4. Use the `system certificate ca` command to install the CA certificate.
5. Use the `system certificate ssh` command to install the SSH certificate. Depending on your terminal software, you can copy the certificate and paste it into the command.

Syntax

```
config system certificate ssh
  edit <name>
    set comment <comment_text>
    set certificate <certificate>
    set private-key <key>
  end
```

Variable	Description
<name>	Enter the SSH certificate name (character limit = 63).
comment <comment_text>	Enter any relevant information about the certificate (character limit = 127).
certificate <certificate>	Enter the signed SSH certificate in PEM format.
You should not modify the following variables if you generated the CSR on this unit.	
private-key <key>	The private key in PEM format.

connector

Use this command to configure connector related settings.

Syntax

```
config system connector
  set conn-refresh-interval <integer>
  set fsso-refresh-interval <integer>
  set fsso-sess-timeout <integer>
  set px-svr-timeout <integer>
end
```

Variable	Description
conn-refresh-interval <integer>	Set the connector refresh interval, in seconds (60 - 1800, default = 300).
fsso-refresh-interval <integer>	Set the FSSO refresh interval, in seconds (60 - 1800, default = 180).
fsso-sess-timeout <integer>	Set the FSSO session timeout, in seconds (30 - 600, default = 300).
px-svr-timeout <integer>	Set the pxGrid session timeout, in seconds (30 - 600, default = 300).

dns

Use these commands to set the DNS server addresses. Several FortiAnalyzer functions, including sending alert email, use DNS. You can configure both IPv4 and IPv6 DNS server addresses.

Syntax

```
config system dns
  set primary <ipv4_address>
  set secondary <ipv4_address>
  set ip6-primary <ipv6_address>
  set ip6-secondary <ipv6_address>
end
```

Variable	Description
primary <ipv4_address>	Enter the primary DNS server IPv4 address.
secondary <ipv4_address>	Enter the secondary DNS IPv4 server address.
ip6-primary <ipv6_address>	Enter the primary DNS server IPv6 address.
ip6-secondary <ipv6_address>	Enter the secondary DNS IPv6 server address.

Example

This example shows how to set the primary FortiAnalyzer DNS server IPv4 address to 172.20.120.99 and the secondary FortiAnalyzer DNS server IPv4 address to 192.168.1.199.

```
config system dns
  set primary 172.20.120.99
  set secondary 192.168.1.199
end
```

docker

Use the following command to enable Docker and management extensions.

Syntax

```
config system docker
  set cpu <integer>
  set default-address-pool_base <ip&netmask>
  set default-address-pool_size <integer>
  set docker-user-login-max <integer>
  set fortisoar {enable | disable}
  set fsmcollector {enable | disable}
  set mem <integer>
  set status {enable | disable | qa | dev}
```

end

Variable	Description
cpu <integer>	Set the maximum % of CPU usage (10 - 50, default = 50).
default-address-pool_base <ip&netmask>	Set the default-address-pool CIDR. Enter the IP address and the netmask (default = 172.17.0.0 255.255.0.0).
default-address-pool_size <integer>	Set the default-address-pool size (default = 24).
docker-user-login-max <integer>	Set the maximum login sessions for the docker users (default = 32).
fortisoar {enable disable}	Enable/disable FortiSOAR (default = disable).
fsmcollector {enable disable}	Enable/disable FSMCollector (default = disable).
mem <integer>	Set the maximum % of RAM usage (10 - 50, default = 50).
status {enable disable qa dev}	Enable/disable Docker and set registry (default = disable): <ul style="list-style-type: none"> • enable: Enable production registry. • disable: Disable the docker host service. • qa: Enable QA test registry. • dev: Enable QA test registry without the signature.

fips

Use this command to set the Federal Information Processing Standards (FIPS) status. FIPS mode is an enhanced security option for some FortiAnalyzer models. Installation of FIPS firmware is required only if the unit was not ordered with this firmware pre-installed.



FIPS mode can only be enabled via console.

Syntax

```
config system fips
  set status enable
  set entropy-token {enable | disable | dynamic}
  set re-seed-interval <integer>
end
```

Variable	Description
status enable	Enable the FIPS-CC mode of operation. Note: enable option is available only via console and when the device is not in FIPS mode.

Variable	Description
entropy-token {enable disable dynamic}	Configure support for the FortiTRNG entropy token when switching to FIPS mode: <ul style="list-style-type: none"> enable: The token must be present during boot up and reseeding. If the token is not present, the boot up or reseeding is interrupted until the token is inserted. disable: The current entropy implementation is used to seed the Random Number Generator (RNG) (default). dynamic: The token is used to seed or reseed the RNG if it is present. If the token is not present, the boot process is not blocked and the old entropy implementation is used.
re-seed-interval <integer>	The amount of time between RNG reseeding, in minutes (0 - 1440, default = 1440).

fortiview

fortiview setting

Use this command to configure FortiView settings.

Syntax

```
config system fortiview setting
    set data-source {auto | cache-only | log-and-cache}
    set not-scanned apps {exclude | include}
    set resolve-ip {enable | disable}
end
```

Variable	Description
data-source {auto cache-only log-and-cache}	Data source of the FortiView query (default = auto): <ul style="list-style-type: none"> auto: Data from hcache and from logs in a flexible way. cache-only: Data from hcache only. log-and-cache: Data from logs and hcache.
not-scanned apps {exclude include}	Include/exclude unscanned applications in FortiView (default = include). Set to exclude to filter out never scanned applications.
resolve-ip {enable disable}	Enable/disable resolving the IP address to the hostname in FortiView (default = disable).

fortiview auto-cache

Use this command to view or configure FortiView auto-cache settings.

Syntax

```
config system fortiview auto-cache
    set aggressive-fortiview {enable | disable}
    set interval <integer>
    set status {enable | disable}
end
```

Variable	Description
aggressive-fortiview {enable disable}	Enable/disable aggressive auto-cache on FortiView (default = disable).
interval <integer>	The time interval for FortiView auto-cache, in hours (default = 168).
status {enable disable}	Enable/disable FortiView auto-cache (default = enable).

global

Use this command to configure global settings that affect miscellaneous FortiAnalyzer features.

Syntax

```
config system global
    set admin-lockout-duration <integer>
    set admin-lockout-threshold <integer>
    set adom-mode {advanced | normal}
    set adom-select {enable | disable}
    set adom-status {enable | disable}
    set backup-compression {high | low | none | normal}
    set backup-to-subfolders {enable | disable}
    set clone-name-option {default | keep}
    set clt-cert-req {enable | disable}
    set console-output {more | standard}
    set contentpack-fgt-install {enable | disable}
    set country-flag {enable | disable}
    set create-revision {enable | disable}
    set daylightsavetime {enable | disable}
    set default-logview-auto-completion {enable | disable}
    set default-search-mode {advanced | filter-based}
    set detect-unregistered-log-device {enable | disable}
    set device-view-mode {regular | tree}
    set disable-module {fortiview-noc | siem | soc}
    set enc-algorithm {custom | high | medium | low}
    set fgfm-ca-cert <certificate>
    set fgfm-local-cert <certificate>
    set fgfm-ssl-protocol {ssl3 | tls1.0 | tls1.1 | tls1.2 | tls1.3}
    set fmg-status {enable | disable}
    set fortirecorder-disk-quota <integer>
    set gui-curl-timeout <integer>
    set gui-polling-interval <integer>
    set ha-member-auto-grouping {enable | disable}
```

```

set hostname <string>
set language {english | japanese | simch | trach}
set latitude <string>
set ldap-cache-timeout <integer>
set ldapconntimeout <integer>
set lock-preempt {enable | disable}
set log-checksum {md5 | md5-auth | none}
set log-forward-cache-size <integer>
set log-mode {analyzer | collector}
set longitude <string>
set max-aggregation-tasks <integer>
set max-log-forward <integer>
set max-running-reports <integer>
set multiple-steps-upgrade-in-autolink {enable | disable}
set no-copy-permission-check {enable | disable}
set normalized-intf-zone-only {enable | disable}
set object-revision-db-max <integer>
set object-revision-mandatory-note {enable | disable}
set object-revision-object-max <integer>
set object-revision-status {enable | disable}
set oftp-ssl-protocol {sslsv3 | tlsv1.0 | tlsv1.1 | tlsv1.2 | tlsv1.3}
set policy-object-icon {enable | disable}
set policy-object-in-dual-pane {enable | disable}
set pre-login-banner {enable | disable}
set pre-login-banner-message <string>
set private-data-encryption {enable | disable}
set remoteauthtimeout <integer>
set search-all-adoms {enable | disable}
config ssl-cipher-suites
    edit <priority>
        set cipher <string>
        set version {tlsv1.2-or-below | tlsv1.3}
    end
set ssl-low-encryption {enable | disable}
set ssl-protocol {tlsv1.3 | tlsv1.2 | tlsv1.1 | tlsv1.0 | sslsv3}
set ssl-static-key-ciphers {enable | disable}
set table-entry-blink {enable | disable}
set task-list-size <integer>
set tftp
set timezone <integer>
set tunnel-mtu <integer>
set usg {enable | disable}
set webservice-proto {tlsv1.3 | tlsv1.2 | tlsv1.1 | tlsv1.0 | sslsv3 | sslsv2}
set workflow-max-sessions <integer>
end

```

Variable	Description
admin-lockout-duration <integer>	Set the lockout duration for FortiAnalyzer administration, in seconds (default = 60).
admin-lockout-threshold <integer>	Set the lockout threshold for FortiAnalyzer administration (1 - 10, default = 3).
adom-mode {advanced normal}	Set the ADOM mode (default = normal).

Variable	Description
adom-select {enable disable}	Enable/disable a pop-up window that allows administrators to select an ADOM after logging in (default = enable).
adom-status {enable disable}	Enable/disable administrative domains (default = disable).
backup-compression {high low none normal}	Set the backup compression level: <code>high</code> (slowest), <code>low</code> (fastest), <code>none</code> , or <code>normal</code> (default).
backup-to-subfolders {enable disable}	Enable/disable the creation of subfolders on server for backup storage (default = disable).
clone-name-option {default keep}	Set the cloned object name option: <ul style="list-style-type: none"> <code>default</code>: Add a Clone of prefix to the name. <code>keep</code>: Keep the original name for the user to edit.
clt-cert-req {enable disable}	Enable/disable requiring a client certificate for GUI login (default = disable). When both <code>clt-cert-req</code> and <code>admin-https-pki-required</code> are enabled, only PKI administrators can connect to the GUI.
console-output {more standard}	Select how the output is displayed on the console (default = standard). Select <code>more</code> to pause the output at each full screen until keypress. Select <code>standard</code> for continuous output without pauses.
contentpack-fgt-install {enable disable}	Enable/disable auto outbreak auto install for FortiGate ADOMs (default = disable).
country-flag {enable disable}	Enable/disable a country flag icon beside an IP address (default = enable).
create-revision {enable disable}	Enable/disable create revision by default (default = disable).
daylightsavetime {enable disable}	Enable/disable daylight saving time (default = enable). If you enable daylight saving time, the FortiAnalyzer unit automatically adjusts the system time when daylight saving time begins or ends.
default-logview-auto-completion {enable disable}	Enable/disable log view filter auto-completion (default = enable).
default-search-mode {advanced filter-based}	Set the default search mode of log view (default = filter-based).
detect-unregistered-log-device {enable disable}	Enable/disable unregistered log device detection (default = enable).
device-view-mode {regular tree}	Set the devices/groups view mode (default = regular).
disable-module {fortiview-noc siem soc}	Disable module list (default = fortirecorder ai).
enc-algorithm {custom high medium low}	Set SSL communication encryption algorithms: <ul style="list-style-type: none"> <code>custom</code>: SSL communication using custom encryption algorithms. <code>high</code>: SSL communication using high encryption algorithms (default). <code>medium</code>: SSL communication using high and medium encryption algorithms. <code>low</code>: SSL communication using all available encryption algorithms.

Variable	Description
fgfm-ca-cert <certificate>	Set the extra FGFM CA certificates ("" = default certificate will be used).
fgfm-local-cert <certificate>	Set the FGFM local certificate ("" = default certificate will be used).
fgfm-ssl-protocol {ssl3 tlsv1.0 tlsv1.1 tlsv1.2 tlsv1.3}	Set the lowest SSL protocols for fgfmsd (default = tlsv1.2).
fmg-status {enable disable}	<p>Disable FortiManager status.</p> <p>If FortiManager features are enabled in FortiAnalyzer before upgrading to 6.2, it will continue to be available after upgrading, and can be disabled with this variable.</p> <p>This variable is only available on some hardware-based FortiAnalyzer devices.</p>
fortirecorder-disk-quota <integer>	<p>Set the disk quota for FortiRecorder, in megabytes (maximum = 8011, default = 3072).</p> <p>This option is only available on hardware devices that support FortiRecorder.</p>
gui-curl-timeout <integer>	Set the GUI cURL timeout in seconds (5-300 default = 30).
gui-polling-interval <integer>	Set the GUI polling interval in seconds (1-288000, default = 5).
ha-member-auto-grouping {enable disable}	Enable/disable automatically grouping HA members when the group name is unique in your network (default = enable).
hostname <string>	FortiAnalyzer host name.
language {english japanese simch spanish trach}	<p>GUI language:</p> <ul style="list-style-type: none"> • <code>english</code>: English (default) • <code>japanese</code>: Japanese • <code>simch</code>: Simplified Chinese • <code>spanish</code>: Spanish • <code>trach</code>: Traditional Chinese
latitude <string>	Set the FortiAnalyzer device's latitude.
ldap-cache-timeout <integer>	LDAP cache timeout, in seconds (default = 86400).
ldapconntimeout <integer>	LDAP connection timeout, in milliseconds (default = 60000).
lock-preempt {enable disable}	Enable/disable the ADOM lock override (default = disable).
log-checksum {md5 md5-auth none}	<p>Record log file hash value, timestamp, and authentication code at transmission or rolling:</p> <ul style="list-style-type: none"> • <code>md5</code>: Record log file's MD5 hash value only. • <code>md5-auth</code>: Record log file's MD5 hash value and authentication code. • <code>none</code>: Do not record the log file checksum (default).
log-forward-cache-size <integer>	Set the log forwarding disk cache size, in gigabytes (default = 30).
log-mode {analyzer collector}	Set the log system operation mode (default = analyzer).
longitude <string>	Set the FortiAnalyzer device's longitude.

Variable	Description
max-aggregation-tasks <integer>	Set the maximum number of concurrent tasks of a log aggregation session (1 - 10, default = 0).
max-log-forward <integer>	Set the maximum log forwarding and aggregation number (5 - 20).
max-running-reports <integer>	Maximum running reports number (1 - 10, default = 1).
multiple-steps-upgrade-in-autolink {enable disable}	Enable/disable multiple steps upgrade in an autolink process (default = disable).
no-copy-permission-check {enable disable}	Do not perform permission check to block object changes in different adom during copy and install (default = disable).
normalized-intf-zone-only {enable disable}	Allow the normalized interface to be zone only (default = disable).
object-revision-db-max <integer>	Maximum revisions for a single database (10000 - 1000000, default = 100000).
object-revision-mandatory-note {enable disable}	Enable/disable mandatory note when creating a revision (default = enable).
object-revision-object-max <integer>	Set the maximum revisions for a single object (10 - 1000, default = 100).
object-revision-status {enable disable}	Enable/disable creating revisions when modifying objects (default = enable).
oftp-ssl-protocol {ssl3 tls1.0 tls1.1 tls1.2 tls1.3}	Set the lowest SSL protocols for oftpd (default = tls1.2).
policy-object-icon {enable disable}	Enable/disable show icons of policy objects (default= disable).
policy-object-in-dual-pane {enable disable}	Enable/disable show policies and objects in dual pane (default= disable).
pre-login-banner {enable disable}	Enable/disable pre-login banner (default= disable).
pre-login-banner-message <string>	Set the pre-login banner message.
private-data-encryption {enable disable}	Enable/disable private data encryption using an AES 128 bit key (default = disable).
remoteauthtimeout <integer>	Remote authentication (RADIUS/LDAP) timeout, in seconds (default = 10).
search-all-adoms {enable disable}	Enable/disable search all ADOMs for where-used queries (default= disable).
ssl-low-encryption {enable disable}	Enable/disable SSL low-grade (40-bit) encryption (default= disable).
ssl-protocol {tls1.3 tls1.2 tls1.1 tls1.0 ssl3}	Set the SSL protocols (default = tls1.3 tls1.2).

Variable	Description
ssl-static-key-ciphers {enable disable}	Enable/disable SSL static key ciphers (default = enable).
table-entry-blink {enable disable}	Enable/disable table entry blink in the GUI (default = enable).
task-list-size <integer>	Set the maximum number of completed tasks to keep (default = 2000).
tftp	
timezone <integer>	The time zone for the FortiManager unit (default = Pacific Time). See Time zones on page 82 .
tunnel-mtu <integer>	Set the maximum transportation unit (68 - 9000, default = 1500).
usg {enable disable}	Enable/disable contacting only FortiGuard servers in the USA (default = enable).
webservice-proto {tls1.2 tls1.1 tls1.0 sslv3 sslv2}	Web Service connection (default = tls1.3 tls1.2).
workflow-max-sessions <integer>	This variable does not function on FortiAnalyzer.
ssl-cipher-suites	Configure the ssl-cipher-suites table to enforce the user specified preferred cipher order in the incoming SSL connections. Note: This command is only available if <code>enc-algorithm</code> is set to <code>custom</code> .
Variables for <code>config ssl-cipher-suites</code> subcommand:	
<priority>	Set the order of the ciphers in the ssl-cipher-suites table.
cipher <string>	Enter the SSL cipher name from the list.
version {tls1.2-or-below tls1.3}	Set the SSL/TLS version the cipher suite can be used with (default = tls1.2-or-below).

Example

The following command turns on daylight saving time, sets the FortiAnalyzer unit name to FMG3k, and chooses the Eastern time zone for US & Canada.

```
config system global
  set daylightsavetime enable
  set hostname FMG3k
  set timezone 12
end
```

Time zones

Integer	Time zone	Integer	Time zone
00	(GMT-12:00) Eniwetak, Kwajalein	40	(GMT+3:00) Nairobi

Integer	Time zone	Integer	Time zone
01	(GMT-11:00) Midway Island, Samoa	41	(GMT+3:30) Tehran
02	(GMT-10:00) Hawaii	42	(GMT+4:00) Abu Dhabi, Muscat
03	(GMT-9:00) Alaska	43	(GMT+4:00) Baku
04	(GMT-8:00) Pacific Time (US & Canada)	44	(GMT+4:30) Kabul
05	(GMT-7:00) Arizona	45	(GMT+5:00) Ekaterinburg
06	(GMT-7:00) Mountain Time (US & Canada)	46	(GMT+5:00) Islamabad, Karachi, Tashkent
07	(GMT-6:00) Central America	47	(GMT+5:30) Calcutta, Chennai, Mumbai, New Delhi
08	(GMT-6:00) Central Time (US & Canada)	48	(GMT+5:45) Kathmandu
09	(GMT-6:00) Mexico City	49	(GMT+6:00) Almaty, Novosibirsk
10	(GMT-6:00) Saskatchewan	50	(GMT+6:00) Astana, Dhaka
11	(GMT-5:00) Bogota, Lima, Quito	51	(GMT+6:00) Sri Jayawardenapura
12	(GMT-5:00) Eastern Time (US & Canada)	52	(GMT+6:30) Rangoon
13	(GMT-5:00) Indiana (East)	53	(GMT+7:00) Bangkok, Hanoi, Jakarta
14	(GMT-4:00) Atlantic Time (Canada)	54	(GMT+7:00) Krasnoyarsk
15	(GMT-4:00) La Paz	55	(GMT+8:00) Beijing, ChongQing, HongKong, Urumqi
16	(GMT-4:00) Santiago	56	(GMT+8:00) Irkutsk, Ulaanbaatar
17	(GMT-3:30) Newfoundland	57	(GMT+8:00) Kuala Lumpur, Singapore
18	(GMT-3:00) Brasilia	58	(GMT+8:00) Perth
19	(GMT-3:00) Buenos Aires, Georgetown	59	(GMT+8:00) Taipei
20	(GMT-3:00) Nuuk (Greenland)	60	(GMT+9:00) Osaka, Sapporo, Tokyo, Seoul
21	(GMT-2:00) Mid-Atlantic	61	(GMT+9:00) Yakutsk
22	(GMT-1:00) Azores	62	(GMT+9:30) Adelaide
23	(GMT-1:00) Cape Verde Is	63	(GMT+9:30) Darwin
24	(GMT) Casablanca, Monrovia	64	(GMT+10:00) Brisbane
25	(GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London	65	(GMT+10:00) Canberra, Melbourne, Sydney
26	(GMT+1:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna	66	(GMT+10:00) Guam, Port Moresby
27	(GMT+1:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague	67	(GMT+10:00) Hobart

Integer	Time zone	Integer	Time zone
28	(GMT+1:00) Brussels, Copenhagen, Madrid, Paris	68	(GMT+10:00) Vladivostok
29	(GMT+1:00) Sarajevo, Skopje, Sofija, Vilnius, Warsaw, Zagreb	69	(GMT+11:00) Magadan
30	(GMT+1:00) West Central Africa	70	(GMT+11:00) Solomon Is., New Caledonia
31	(GMT+2:00) Athens, Istanbul, Minsk	71	(GMT+12:00) Auckland, Wellington
32	(GMT+2:00) Bucharest	72	(GMT+12:00) Fiji, Kamchatka, Marshall Is
33	(GMT+2:00) Cairo	73	(GMT+13:00) Nuku'alofa
34	(GMT+2:00) Harare, Pretoria	74	(GMT-4:30) Caracas
35	(GMT+2:00) Helsinki, Riga, Tallinn	75	(GMT+1:00) Namibia
36	(GMT+2:00) Jerusalem	76	(GMT-5:00) Brazil-Acre)
37	(GMT+3:00) Baghdad	77	(GMT-4:00) Brazil-West
38	(GMT+3:00) Kuwait, Riyadh	78	(GMT-3:00) Brazil-East
39	(GMT+3:00) Moscow, St.Petersburg, Volgograd	79	(GMT-2:00) Brazil-DeNoronha

ha

Use this command to enable and configure FortiAnalyzer high availability (HA).

FortiAnalyzer HA clusters provide real-time redundancy in case a unit fails. Logs, data, and relevant system settings are securely synchronized across multiple FortiAnalyzer devices, and processing tasks can be shared to alleviate the load on the primary unit.

A FortiAnalyzer HA cluster can have a maximum of four units, all of which are visible on the network. All of the units must be from the same product series and in the same operating mode (analyzer or collector). HA is not supported when FortiManager features are enabled.

For more information, see the [FortiAnalyzer Administration Guide](#).

Syntax

```
config system ha
  set cfg-sync-hb-interval <integer>
  set group-id <integer>
  set group-name <name>
  set hb-interface <string>
  set hb-interval <integer>
  set healthcheck {DB | fault-test}
  set initial-sync {true | false}
  set initial-sync-threads <integer>
  set load-balance {disable | round-robin}
```

```

set log-sync {enable | disable}
set mode {a-p | standalone}
set password <passwd>
set preferred-role
set priority <integer>
set unicast {enable | disable}
config peer
    edit <peer_id_int>
        set ip <peer_ip_address>
        set ip-hb <string>
        set serial-number <string>
        set status {enable | disable}
    end
config vip
    edit <id>
        set status {enable | disable}
        set vip <string>
        set vip-interface <string>
    end
end
end

```

Variable	Description
cfg-sync-hb-interval <integer>	Configure the sync heartbeat interval (1 - 255, default = 3).
group-id <integer>	Set the HA group ID (1 - 255, default = 0).
group-name <name>	Set the HA group name.
hb-interface <string>	Set the interface for the heartbeat.
hb-interval <integer>	The time, in seconds, that a cluster unit waits between sending heartbeat packets. The heartbeat interval is also the amount of time that a cluster unit waits before expecting to receive a heartbeat packet from the other cluster unit (1 - 20, default = 1).
healthcheck {DB fault-test}	Set the healthcheck options: <ul style="list-style-type: none"> DB - Check that the database is running. fault-test - Temp fault test.
initial-sync {true false}	Synchronize data from the primary device before joining the HA cluster (default = true).
initial-sync-threads <integer>	Number of threads used for initial synchronization (1 - 15, default = 4).
load-balance {disable round-robin}	Configure load balancing to secondary units (default = round-robin).
log-sync {enable disable}	Synchronize logs to backup FortiAnalyzer devices (default = enable).
mode {a-p standalone}	Set the HA operating mode: Active-passive mode (a-p) or Standalone mode (standalone) (default = standalone).
password <passwd>	Set the HA group password.
priority <integer>	Set the runtime priority (80 - 120, default = 100).

Variable	Description
preferred-role {primary secondary}	The preferred role of this unit (default = secondary). The runtime role may be different.
unicast {enable disable}	Enable/disable unicast for HA heartbeat (default = disable).
Variables for <code>vip</code> subcommand:	
status {enable disable}	Enable/disable virtual ip status (default = enable).
vip <string>	Set the virtual IP address for the HA cluster.
vip-interface <string>	Set the virtual interface for configuring the virtual IP address.
Variables for <code>config peer</code> subcommand:	
<peer_id_int>	Add a peer and add the peer's IPv4 or IPv6 address and serial number.
ip <peer_ip_address>	Enter the IPv4 address of the peer FortiAnalyzer unit.
ip-hb <string>	Enter the IP address of the peer's VIP interface for heartbeat. This only needs to be set if the value is different than the peer's IP address, and is only needed when using unicast.
serial-number <string>	Enter the serial number of the peer FortiAnalyzer unit.
status {enable disable}	Enter the status of the peer FortiAnalyzer unit (default = enable).

interface

Use this command to edit the configuration of a FortiAnalyzer network interface.

Syntax

```
config system interface
  edit <port_string>
    set status {enable | disable}
    set ip <ipv4address_mask>
    set allowaccess {fgfm http https https-logging ping snmp soc-fabric ssh webservice}
    set speed {1000full | 100full | 100half | 10full | 10half | auto}
    set description <string>
    set alias <string>
    set mtu <integer>
    set type {aggregate | physical}
    config member
      edit <interface-name>
    end
    set lacp-mode
    set lacp-speed {fast | slow}
    set min-links <integer>
    set min-links-down {administrative | operational}
    set link-up-delay <integer>
    set aggregate
```

```

    set camera-discovery {enable | disable}
    config ipv6
        set ip6-address <IPv6address prefix>
        set ip6-allowaccess {fgfm http https https-logging ping snmp ssh webservice}
        set ip6-autoconf {enable | disable}
    end
end

```

Variable	Description
<port>	The port can be set to a port number such as port1, port2, port3, or port4. Different FortiAnalyzer models have different numbers of ports.
status {enable disable}	Enable/disable the interface (default = enable). If the interface is disabled it does not accept or send packets. If you disable a physical interface, VLAN interfaces associated with it are also disabled.
ip <ipv4_mask>	Enter the interface IPv4 address and netmask. The IPv4 address cannot be on the same subnet as any other interface.
allowaccess {fgfm http https https-logging ping snmp soc-fabric ssh webservice}	Enter the types of management access permitted on this interface. Separate multiple selected types with spaces. If you want to add or remove an option from the list, retype the list as required.
speed {1000full 100full 100half 10full 10half auto}	Enter the speed and duplexing the network port uses: <ul style="list-style-type: none"> 100full: 100M full-duplex 100half: 100M half-duplex 10full: 10M full-duplex 10half: 10M half-duplex auto: Automatically negotiate the fastest common speed (default)
description <string>	Enter a description of the interface (character limit = 63).
alias <string>	Enter an alias for the interface.
mtu <integer>	Set the maximum transportation unit (68 - 9000, default = 1500).
type {aggregate physical}	Set the type of interface (default = aggregate).
member	Physical interfaces that belong to the aggregate or the redundant interface.
lACP-mode	Set the mode for LACP messages (default = active).
lACP-speed {fast slow}	Set how often the interface sends LACP messages: <ul style="list-style-type: none"> fast: Send LACP message every second. slow: Send LACP message every 30 seconds (default).
min-links <integer>	Set the minimum number of aggregated ports that must be up (default = 1).
min-links-down {administrative operational}	Action to take when less than the configured minimum number of links are active: <ul style="list-style-type: none"> administrative: Set the aggregate administratively down. operational: Set the aggregate operationally down (default).
link-up-delay <integer>	Set the number of milliseconds to wait before considering a link is up (default = 50).

Variable	Description
aggregate	
camera-discovery {enable disable}	Enable/disable camera discovery (default = enable). This option is only available on hardware devices that support FortiRecorder.
ipv6	IPv6 of the interface.
Variables for <code>member</code> subcommand:	
<interface-name>	Enter the interface name.
Variables for <code>ipv6</code> subcommand:	
ip6-address <ip6 prefix>	IPv6 address/prefix of interface.
ip6-allowaccess {fgfm http https https-logging ping snmp ssh webservice}	Allow management access to the interface.
ip6-autoconf {enable disable}	Enable/disable address automatic configuration (SLAAC) (default = enable).

Example

This example shows how to set the FortiAnalyzer port1 interface IPv4 address and network mask to 192.168.100.159 255.255.255.0, and the management access to ping, https, and ssh.

```
config system interface
  edit port1
    set allowaccess ping https ssh
    set ip 192.168.110.26 255.255.255.0
    set status up
  end
```

locallog

Use the following commands to configure local log settings.

locallog setting

Use this command to configure locallog logging settings.

Syntax

```
config system locallog setting
  set log-interval-dev-no-logging <integer>
  set log-interval-disk-full <integer>
  set log-interval-gbday-exceeded <integer>
end
```


Variable	Description
log-interval-dev-no-logging <integer>	Interval for logging the event of no logs received from a device, in minutes (default = 1400).
log-interval-disk-full <integer>	Interval for logging the event of disk full, in minutes (default = 5).
log-interval-gbday-exceeded <integer>	Interval for logging the event of the GB/Day license exceeded, in minutes (default = 1400).

locallog disk setting

Use this command to configure the disk settings for uploading log files, including configuring the severity of log levels.

- status must be enabled to view diskfull, max-log-file-size and upload variables.
- upload must be enabled to view/set other upload* variables.

Syntax

```
config system locallog disk setting
    set status {enable | disable}
    set severity {emergency | alert | critical | error | warning | notification |
        information | debug}
    set max-log-file-size <integer>
    set max-log-file-num <integer>
    set roll-schedule {none | daily | weekly}
    set roll-day <string>
    set roll-time <hh:mm>
    set diskfull {nolog | overwrite}
    set log-disk-full-percentage <integer>
    set log-disk-quota <integer>
    set upload {enable | disable}
    set uploadip <ipv4_address>
    set server-type {FAZ | FTP | SCP | SFTP}
    set uploadport <integer>
    set uploaduser <string>
    set uploadpass <passwd>
    set uploadaddr <string>
    set uploadtype <event>
    set uploadzip {enable | disable}
    set uploadsched {enable | disable}
    set upload-time <hh:mm>
    set upload-delete-files {enable | disable}
end
```

Variable	Description
status {enable disable}	Enable/disable logging to the local disk (default = enable)
severity {emergency alert critical error warning notification information debug }	Select the logging severity level. The FortiAnalyzer unit logs all messages at and above the logging severity level you select.

Variable	Description
	<ul style="list-style-type: none"> emergency: The unit is unusable. alert: Immediate action is required. critical: Functionality is affected. error: Functionality is probably affected. warning: Functionality might be affected. notification: Information about normal events. information: General information about unit operations (default). debug: Information used for diagnosis or debugging.
max-log-file-size <integer>	Enter the size at which the log is rolled, in megabytes (1 - 1024, default = 100).
max-log-file-num <integer>	Enter the number of log files at which the logs are rolled (10 - 10000, default = 10000).
roll-schedule {none daily weekly}	Enter the period for the scheduled rolling of a log file: <ul style="list-style-type: none"> none: Not scheduled; the log rolls when max-log-file-size is reached (default). daily: Every day. weekly: Every week.
roll-day {sunday monday tuesday wednesday thursday friday saturday}	Enter the day for the scheduled rolling of a log file (default = sunday).
roll-time <hh:mm>	Enter the time for the scheduled rolling of a log file.
diskfull {nolog overwrite}	Enter action to take when the disk is full: <ul style="list-style-type: none"> nolog: stop logging overwrite: overwrites oldest log entries (default)
log-disk-full-percentage <integer>	Enter the percentage at which the log disk will be considered full (50 - 90, default = 80).
log-disk-quota <integer>	Enter the quota for controlling local log size, in GB (0 - 25, default = 5). Note: 0 means no control of local log size.
upload {enable disable}	Enable/disable uploading of logs when rolling log files (default = disable).
uploadip <ipv4_address>	Enter IPv4 address of the destination server.
server-type {FTP SCP SFTP}	Enter the server type to use to store the logs: <ul style="list-style-type: none"> FTP: upload via FTP (default) SCP: upload via SCP SFTP: upload via SFTP
uploadport <integer>	Enter the port to use when communicating with the destination server (1 - 65535, default = 0).
uploaduser <string>	Enter the user account on the destination server.
uploadpass <passwd>	Enter the password of the user account on the destination server (character limit = 127).

Variable	Description
uploaddir <string>	Enter the destination directory on the remote server.
uploadtype <event>	Enter to upload the event log files (default = event).
uploadzip {enable disable}	Enable to compress uploaded log files (default = disable).
uploadsched {enable disable}	Enable to schedule log uploads (default = disable).
upload-time <hh:mm>	Enter to configure when to schedule an upload.
upload-delete-files {enable disable}	Enable/disable deleting log files after uploading (default = enable).

Example

In this example, the logs are uploaded to an upload server and are not deleted after they are uploaded.

```
config system locallog disk setting
  set status enable
  set severity information
  set max-log-file-size 1000MB
  set roll-schedule daily
  set upload enable
  set uploadip 10.10.10.1
  set uploadport port 443
  set uploaduser myname2
  set uploadpass 12345
  set uploadtype event
  set uploadzip enable
  set uploadsched enable
  set upload-time 06:45
  set upload-delete-file disable
end
```

locallog filter

Use this command to configure filters for local logs. All keywords are visible only when `event` is enabled.

Syntax

```
config system locallog [disk | memory | fortianalyzer | fortianalyzer2 | fortianalyzer3 |
  syslogd | syslogd2 | syslogd3] filter
  set aid {enable | disable}
  set controller {enable | disable}
  set devcfg {enable | disable}
  set devops {enable | disable}
  set diskquota {enable | disable}
  set dm {enable | disable}
  set docker {enable | disable}
  set dvm {enable | disable}
  set ediscovery {enable | disable}
  set epmgr {enable | disable}
```

```

set event {enable | disable}
set eventmgmt {enable | disable}
set faz {enable | disable}
set fazha {enable | disable}
set fazsys {enable | disable}
set fgd {enable | disable}
set fgfm {enable | disable}
set fips {enable | disable}
set fmgws {enable | disable}
set fmlmgr {enable | disable}
set fmwmgr {enable | disable}
set fortiview {enable | disable}
set glbcfg {enable | disable}
set ha {enable | disable}
set hcache {enable | disable}
set incident {enable | disable}
set iolog {enable | disable}
set logd {enable | disable}
set logdb {enable | disable}
set logdev {enable | disable}
set logfile {enable | disable}
set logging {enable | disable}
set lrmgr {enable | disable}
set objcfg {enable | disable}
set report {enable | disable}
set rev {enable | disable}
set rtmon {enable | disable}
set scfw {enable | disable}
set scply {enable | disable}
set scrmgr {enable | disable}
set scvpn {enable | disable}
set system {enable | disable}
set webport {enable | disable}
end

```

Variable	Description
aid {enable disable}	Enable/disable configuring aid messages (default = enable).
controller {enable disable}	Enable/disable controller application generic messages (default = enable).
devcfg {enable disable}	Enable/disable logging device configuration messages (default = enable).
devops {enable disable}	Enable/disable managed device's operations messages (default = enable).
diskquota {enable disable}	Enable/disable logging FortiAnalyzer disk quota messages (default = enable).
dm {enable disable}	Enable/disable logging deployment manager messages (default = enable).
docker {enable disable}	Enable/disable docker application generic messages (default = enable).
dvm {enable disable}	Enable/disable logging device manager messages (default = enable).
ediscovery {enable disable}	Enable/disable logging device manager messages (default = enable).
epmgr {enable disable}	Enable/disable logging endpoint manager messages (default = enable).
event {enable disable}	Enable/disable configuring log filter messages (default = enable).

Variable	Description
eventmgmt {enable disable}	Enable/disable logging FortiAnalyzer event handler messages (default = enable).
faz {enable disable}	Enable/disable logging FortiAnalyzer messages (default = enable).
fazha {enable disable}	Enable/disable logging FortiAnalyzer HA messages (default = enable).
fazsys {enable disable}	Enable/disable logging FortiAnalyzer system messages (default = enable).
fgd {enable disable}	Enable/disable logging FortiGuard service messages (default = enable).
fgfm {enable disable}	Enable/disable logging FortiGate/FortiManager communication protocol messages (default = enable).
fips {enable disable}	Enable/disable logging FIPS messages (default = enable).
fmgws {enable disable}	Enable/disable logging web service messages (default = enable).
fmlmgr {enable disable}	Enable/disable logging FortiMail manager messages (default = enable).
fmwmgr {enable disable}	Enable/disable logging firmware manager messages (default = enable).
fortiview {enable disable}	Enable/disable logging FortiAnalyzer FortiView messages (default = enable).
glbcfg {enable disable}	Enable/disable logging global database messages (default = enable).
ha {enable disable}	Enable/disable logging high availability activity messages (default = enable).
hcache {enable disable}	Enable/disable logging hcache messages (default = enable).
incident {enable disable}	Enable/disable logging FortiAnalyzer incident messages (default = enable).
iolog {enable disable}	Enable/disable input/output log activity messages (default = enable).
logd {enable disable}	Enable/disable logd messages (default = enable).
logdb {enable disable}	Enable/disable logging FortiAnalyzer log DB messages (default = enable).
logdev {enable disable}	Enable/disable logging FortiAnalyzer log device messages (default = enable).
logfile {enable disable}	Enable/disable logging FortiAnalyzer log file messages (default = enable).
logging {enable disable}	Enable/disable logging FortiAnalyzer logging messages (default = enable).
lrmgr {enable disable}	Enable/disable logging log and report manager messages (default = enable).
objcfg {enable disable}	Enable/disable logging object configuration (default = enable).
report {enable disable}	Enable/disable logging FortiAnalyzer report messages (default = enable).
rev {enable disable}	Enable/disable logging revision history messages (default = enable).
rtmon {enable disable}	Enable/disable logging real-time monitor messages (default = enable).
scfw {enable disable}	Enable/disable logging firewall objects messages (default = enable).
scply {enable disable}	Enable/disable logging policy console messages (default = enable).
scrmgr {enable disable}	Enable/disable logging script manager messages (default = enable).
scvpn {enable disable}	Enable/disable logging VPN console messages (default = enable).

Variable	Description
system {enable disable}	Enable/disable logging system manager messages (default = enable).
webport {enable disable}	Enable/disable logging web portal messages (default = enable).

Example

In this example, the local log filters are log and report manager, and system settings. Events in these areas of the FortiAnalyzer unit will be logged.

```
config system locallog filter
    set event enable
    set lrmgr enable
    set system enable
end
```

locallog fortianalyzer (fortianalyzer2, fortianalyzer3) setting

Use this command to enable or disable, and select the severity threshold of, remote logging to the FortiAnalyzer units. You can configure up to three FortiAnalyzer devices.

The severity threshold required to forward a log message to the FortiAnalyzer unit is separate from event, syslog, and local logging severity thresholds.

Syntax

```
config system locallog {fortianalyzer | fortianalyzer2 | fortianalyzer3} setting
    set peer-cert-cn <string>
    set reliable {enable | disable}
    set secure-connection {enable | disable}
    set server <address>
    set severity {emergency | alert | critical | error | warning | notification |
        information | debug}
    set status {disable | realtime | upload}
    set upload-time <hh:mm>
end
```

Variable	Description
peer-cert-cn <string>	Certificate common name for the remote FortiAnalyzer. This variable is available only when the status is upload. Note: Null or '-' means no certificate CN for the remote FortiAnalyzer. Multiple CNs are separated by commas. If there is comma in CN, it must follow an escape character.
reliable {enable disable}	Enable/disable reliable realtime logging (default = disable).
secure-connection {enable disable}	Enable/disable connection secured by TLS/SSL (default = disable). This variable is available when <code>status</code> is <code>realtime</code> or <code>upload</code> .

Variable	Description
server <address>	Remote FortiAnalyzer server IP address, FQDN, or hostname.
severity {emergency alert critical error warning notification information debug }	Select the logging severity level (default = notification). The FortiAnalyzer unit logs all messages at and above the logging severity level you select.
status {disable realtime upload}	Set the log to FortiAnalyzer status: <ul style="list-style-type: none"> • disable: Do not log to FortiAnalyzer (default). • realtime: Log to FortiAnalyzer in realtime. • upload: Log to FortiAnalyzer at a scheduled time.
upload-time <hh:mm>	Set the time to upload local log files (default = 00:00).

Example

You might enable remote logging to the FortiAnalyzer unit configured. Events at the information level and higher, which is everything except debug level events, would be sent to the FortiAnalyzer unit.

```
config system locallog fortianalyzer setting
  set status enable
  set severity information
end
```

locallog memory setting

Use this command to configure memory settings for local logging purposes.

Syntax

```
config system locallog memory setting
  set diskfull {nolog | overwrite}
  set severity {emergency | alert | critical | error | warning | notification |
    information | debug}
  set status <enable | disable>
end
```

Variable	Description
diskfull {nolog overwrite}	Enter the action to take when the disk is full: <ul style="list-style-type: none"> • nolog: Stop logging when disk full • overwrite: Overwrites oldest log entries
severity {emergency alert critical error warning notification information debug}	Select the logging severity level (default = notification). The FortiAnalyzer unit logs all messages at and above the logging severity level you select.
status <enable disable>	Enable/disable logging to the memory buffer (default = disable).

Example

This example shows how to enable logging to memory for all events at the notification level and above. At this level of logging, only information and debug events will not be logged.

```
config system locallog memory
    set severity notification
    set status enable
end
```

locallog syslogd (syslogd2, syslogd3) setting

Use this command to configure the settings for logging to a syslog server. You can configure up to three syslog servers: syslogd, syslogd2 and syslogd3.

Syntax

```
config system locallog {syslogd | syslogd2 | syslogd3} setting
    set cert {Fortinet_Local | Fortinet_Local2}
    set csv {enable | disable}
    set facility {alert | audit | auth | authpriv | clock | cron | daemon | ftp | kernel |
        local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7 | lpr |
        mail | news | ntp | syslog | user | uucp}
    set reliable {enable | disable}
    set secure-connection {enable | disable}
    set severity {emergency | alert | critical | error | warning | notification |
        information | debug}
    set status {enable | disable}
    set syslog-name <string>
end
```

Variable	Description
cert {Fortinet_Local Fortinet_Local2}	Select local certificate used for secure connection.
csv {enable disable}	Enable/disable producing the log in comma separated value (CSV) format (default = disable). If you do not enable CSV format the FortiAnalyzer unit produces space separated log files.
facility {alert audit auth authpriv clock cron daemon ftp kernel local0 local1 local2 local3 local4 local5 local6 local7 lpr mail news ntp syslog user uucp}	Enter the facility type (default = local7). The facility identifies the source of the log message to syslog. Change <i>facility</i> to distinguish log messages from different FortiAnalyzer units so you can determine the source of the log messages. <i>local0</i> to <i>local7</i> are reserved for local use.
reliable {enable disable}	Enable/disable reliable real time logging (default = disable).
secure-connection {enable disable}	Enable/disable connection secured by TLS/SSL (default = disable). This variable is available only when <i>reliable</i> is enabled.

Variable	Description
severity {emergency alert critical error warning notification information debug}	Select the logging severity level (default = notification). The FortiAnalyzer unit logs all messages at and above the logging severity level you select.
status {enable disable}	Enable/disable logging to the remote syslog server (default = disable).
syslog-name <string>	Enter the remote syslog server name. To configure a syslog server, use the <code>config system syslog</code> command. See syslog on page 134 for information.

Use the show command to display the current configuration if it has been changed from its default value:

```
show system locallog syslogd setting
```

Example

In this example, the logs are uploaded to a previously configured syslog server named `logstorage`. The FortiAnalyzer unit is identified as facility `local0`.

```
config system locallog syslogd setting
  set facility local0
  set syslog-name logstorage
  set status enable
  set severity information
end
```

log

Use the following commands to configure log settings.

log alert

Use this command to configure log based alert settings.

Syntax

```
config system log alert
  set max-alert-count <integer>
end
```

Variable	Description
max-alert-count <integer>	Maximum number of alerts supported (100 - 50000, default = 10000).

log device-disable

Use this command to disable the client device logging.

Syntax

```
config system log device-disable
  edit <id>
    set device <string>
    set TTL <string>
  end
```

Variable	Description
<id>	The device ID.
device <string>	The device ID to be used for disabling logging. Note: The device ID is not checked against the currently registered devices in the system. The entered device ID is ignored if no match is found.
TTL <string>	Set the duration for Time to Live (TTL). For instance, enter 1d5h for 1 day and 5 hours. Supported units: <ul style="list-style-type: none">• d- day.• h- hour.• m- minute.• s- second. Leave the field unset for no expiration. Note: Do not input auto generated part from [expire:..

fos-policy-stats

Use this command to configure FortiOS policy statistics settings.

Syntax

```
config system log fos-policy-stats
  set retention-days <integer>
  set sampling-interval <integer>
  set status{enable | disable}
end
```

Variable	Description
retention-days <integer>	The number of days that FortiOS policy stats are stored (60 - 1825, default = 365).
sampling-interval <integer>	The interval in which policy stats data are received from FortiOS devices, in minutes (5 - 1440, default = 60).
status {enable disable}	Enable/disable FortiOS policy statistics feature (default = enable).

log interface-stats

Use this command to configure log based interface statistics settings.

Syntax

```
config system log interface-stats
  set billing-report {enable | disable}
  set retention-days <integer>
  set sampling-interval <integer>
  set status {enable | disable}
end
```

Variable	Description
billing-report {enable disable}	Enable/disable billing report feature (default = disable).
retention-days <integer>	The number of days that interface data are stored (0 - 2000, default = 100).
sampling-interval <integer>	The interval in which interface data are received from FortiGate devices, in seconds (300 - 86400, default = 1200).
status {enable disable}	Enable/disable interface statistics (default = enable).

log ioc

Use this command to configure log based IoC (Indicators of Compromise) settings.

Syntax

```
config system log ioc
  set notification {enable | disable}
  set notification-throttle <integer>
  set rescan-max-runner <integer>
  set rescan-run-at <integer>
  set rescan-status {enable | disable}
  set status {enable | disable}
end
```

Variable	Description
notification {enable disable}	Enable/disable IoC notification (default = enable).
notification-throttle <integer>	Set the minute value for throttling the rate of IoC notifications (1 - 10080, default = 1440).
rescan-max-runner <integer>	Set the maximum number of concurrent IoC rescans (1 to CPU count, default = 8).

Variable	Description
rescan-run-at <integer>	Set the hour of the day when IoC rescan runs (1 - 24, 0 = run immediately, default = 24).
rescan-status {enable disable}	Enable/disable IoC rescan (default = enable).
status {enable disable}	Enable/disable the IoC feature (default = enable).

log mail-domain

Use this command to configure FortiMail domain settings.

Syntax

```
config system log mail-domain
  edit <id>
    set devices <string>
    set domain <string>
    set vdom <string>
  end
```

Variable	Description
<id>	The ID of the FortiMail domain.
devices <string>	The device IDs for domain to VDOM mapping, separated by commas (default = All_FortiMails). For example: FEVM020000000000, FEVM020000000001
domain <string>	The FortiMail domain.
vdom <string>	The VDOM name that is mapping to the FortiMail domain.

log ratelimit

Use this command to log the rate limit.

Syntax

```
config system log ratelimit
  set device-ratelimit-default <integer>
  set mode {disable | manual}
  set system-ratelimit <integer>
  config ratelimits
    edit id
      set filter <string>
      set filter-type {adom | devid}
      set ratelimit <integer>
    end
  end
```

Variable	Description
device-ratelimit-default <integer>	The default maximum device log rate limit (default = 0). Note: This command is only available when the mode is set to <code>manual</code> .
mode {disable manual}	The logging rate limit mode (default = disable). In the manual mode, the system rate limit and the device rate limit both are configurable, no limit if not configured.
system-ratelimit <integer>	The maximum system log rate limit (default = 0). Note: This command is only available when the mode is set to <code>manual</code> .
ratelimits	The device log rate limit.
Variables for <code>config ratelimits</code> subcommand:	
<id>	The device id.
filter <string>	The device(s) or ADOM filter according to the filter-type setting. Note: Wildcard expression is supported.
filter-type { adom devid}	The device filter type (default = devid): <ul style="list-style-type: none"> • adom: ADOM name. • devid: Device ID.
ratelimit <integer>	The maximum device log rate limit (default = 0).

log settings

Use this command to configure settings for logs.

Syntax

```
config system log settings
  set browse-max-logfiles <integer>
  set device-auto-detect {enable | disable}
  set dns-resolve-dstip {enable | disable}
  set download-max-logs <integer>
  set FAC-custom-field1 <string>
  set FAZ-custom-field1 <string>
  set FCH-custom-field1 <string>
  set FCT-custom-field1 <string>
  set FDD-custom-field1 <string>
  set FGT-custom-field1 <string>
  set FMG-custom-field1 <string>
  set FML-custom-field1 <string>
  set FPX-custom-field1 <string>
  set FSA-custom-field1 <string>
  set FWB-custom-field1 <string>
  set ha-auto-migrate {enable | disable}
  set import-max-logfiles <integer>
  set keep-dev-logs {enable | disable}
```

```

set log-file-archive-name {basic | extended}
set sync-search-timeout <integer>
set unencrypted-logging {enable | disable}
config {rolling-regular | rolling-local | rolling-analyzer}
    set days {fri | mon | sat | sun | thu | tue | wed}
    set del-files {enable | disable}
    set directory <string>
    set file-size <integer>
    set gzip-format {enable | disable}
    set hour <integer>
    set ip <ipv4_address>
    set ip2 <ipv4_address>
    set ip3 <ipv4_address>
    set log-format {csv | native | text}
    set min <integer>
    set password <passwd>
    set password2 <passwd>
    set password3 <passwd>
    set port <integer>
    set port2 <integer>
    set port3 <integer>
    set rolling-upgrade-status <integer>
    set server-type {ftp | scp | sftp}
    set upload {enable | disable}
    set upload-hour <integer>
    set upload-mode {backup | mirror}
    set upload-trigger {on-roll | on-schedule}
    set username <string>
    set username2 <string>
    set username3 <string>
    set when {daily | none | weekly}
end
end

```

Variable	Description
browse-max-logfiles <integer>	Maximum number of log files for each log browse attempt, per ADOM (default = 10000).
device-auto-detect {enable disable}	Enable/disable looking up device ID in syslog received with no encryption (default = enable).
dns-resolve-stip {enable disable}	Enable/disable resolving destination IP by DNS (default = disable).
download-max-logs <integer>	Maximum number of logs for each log download attempt (default = 100000).
FAC-custom-field1 <string>	Enter a name of the custom log field to index (character limit = 31).
FAZ-custom-field1 <string>	Enter a name of the custom log field to index (character limit = 31).
FCH-custom-field1 <string>	Enter a name of the custom log field to index (character limit = 31).
FCT-custom-field1 <string>	Enter a name of the custom log field to index (character limit = 31).
FDD-custom-field1 <string>	Enter a name of the custom log field to index (character limit = 31).

Variable	Description
FGT-custom-field1 <string>	Enter a name of the custom log field to index (character limit = 31).
FMG-custom-field1 <string>	Enter a name of the custom log field to index (character limit = 31).
FML-custom-field1 <string>	Enter a name of the custom log field to index (character limit = 31).
FPX-custom-field1 <string>	Enter a name of the custom log field to index (character limit = 31).
FSA-custom-field1 <string>	Enter a name of the custom log field to index (character limit = 31).
FWB-custom-field1 <string>	Enter a name of the custom log field to index (character limit = 31).
ha-auto-migrate {enable disable}	Enabled/disable automatically merging HA member's logs to HA cluster (default = disable).
import-max-logfiles <integer>	Maximum number of log files for each log import attempt (default = 10000).
keep-dev-logs {enable disable}	Enable/disable keeping the device logs after the device has been deleted (default = disable).
log-file-archive-name {basic extended}	Log file name format for archiving. <ul style="list-style-type: none"> • basic: Basic format for log archive file name (default), for example: FGT20C0000000001.tlog.1417797247.log. • extended: Extended format for log archive file name, for example: FGT20C0000000001.2014-12-05-08:34:58.tlog.1417797247.log.
sync-search-timeout <integer>	The maximum amount of time that a log search session can run in synchronous mode, in seconds (1 - 86400, default = 60).
unencrypted-logging {enable disable}	Enable/disable receiving syslog through UDP(514) or TCP(514) un-encrypted (default = disable).
Variables for config {rolling-regular rolling-local rolling-analyzer} subcommand:	
days {fri mon sat sun thu tue wed}	Log files rolling schedule (days of the week). When <code>when</code> is set to <code>weekly</code> , you can configure <code>days</code> , <code>hour</code> , and <code>min</code> values.
del-files {enable disable}	Enable/disable log file deletion after uploading (default = disable).
directory <string>	The upload server directory (character limit = 127).
file-size <integer>	Roll log files when they reach this size, in megabytes (10 - 1000, default = 200).
gzip-format {enable disable}	Enable/disable compression of uploaded log files (default = disable).
hour <integer>	The hour of the day that log files are rolled (0 - 23, default = 0).
ip <ipv4_address> ip2 <ipv4_address> ip3 <ipv4_address>	Upload server IPv4 addresses. Configure up to three servers.
log-format {csv native text}	Format of uploaded log files: <ul style="list-style-type: none"> • csv: CSV (comma-separated value) format. • native: Native format (text or compact) (default). • text: Text format (convert if necessary).

Variable	Description
min <integer>	The minute of the hour that log files are rolled (0 - 59, default = 0).
password <passwd> password2 <passwd> password3 <passwd>	Upload server log in passwords (character limit = 128).
port <integer> port2 <integer> port3 <integer>	Upload server IP port number.
rolling-upgrade-status <integer>	The rolling upgrade status.
server-type {ftp scp sftp}	Upload server type (default = ftp).
upload {enable disable}	Enable/disable log file uploads (default = disable).
upload-hour <integer>	The hour of the day that log files are uploaded (0 - 23, default = 0).
upload-mode {backup mirror}	Configure upload mode with multiple servers. Servers are tried then used one after the other upon failure to connect. <ul style="list-style-type: none"> backup: Servers are attempted and used one after the other upon failure to connect (default). mirror: All configured servers are attempted and used.
upload-trigger {on-roll on-schedule}	Event triggering log files upload: <ul style="list-style-type: none"> on-roll: Upload log files after they are rolled (default). on-schedule: Upload log files daily.
username <string> username2 <string> username3 <string>	Upload server log in usernames (character limit = 35).
when {daily none weekly}	Roll log files periodically: <ul style="list-style-type: none"> daily: Roll log files daily. none: Do not roll log files periodically . weekly: Roll log files on certain days of week (default).

log topology

Use this command to configure settings for the logging topology.

Syntax

```
config system log topology
    set max-depth <integer>
    set max-depth-share <integer>
end
```


Variable	Description
max-depth <integer>	Maximum levels to descend from this device to get the logging topology information (0 - 32, default = 5).
max-depth-share <integer>	Maximum levels to descend from this device to share logging topology information with upstream (0 - 32, default = 5).

log-fetch

Use the following commands to configure log fetching.

log-fetch client-profile

Use this command to configure the fetching client settings.

Syntax

```
config system log-fetch client-profile
  edit <id>
    set client-adom <string>
    set data-range {custom}
    set data-range-value <integer>
    set end-time <hh:mm> <yyyy/mm/dd>
    set index-fetch-logs {enable | disable}
    set log-filter-status {enable | disable}
    set log-filter-logic {and | or}
    set name <string>
    set password <passwd>
    set peer-cert-cn <string>
    set secure-connection {enable | disable}
    set server-adom <string>
    set server-ip <ip>
    set start-time <hh:mm> <yyyy/mm/dd>
    set sync-adom-config {enable | disable}
    set user <string>
    config device-filter
      edit <id>
        set adom <string>
        set device <device>
        set vdom <string>
      next
    config log-filter
      edit <id>
        set field <string>
        set oper {= | != | < | > | <= | >= | contain | not-contain | match}
        set value <string>
      next
    next
  end
```

end

Variable	Description
<id>	The log-fetch client profile ID.
client-adom <string>	Log-fetch client side's adom name.
data-range {custom}	The data range settings for the fetched logs, which is always custom.
data-range-value <integer>	An integer representing the data range value.
end-time <hh:mm> <yyyy/mm/dd>	Set the end date and time of the data-range.
index-fetch-logs {enable disable}	Enable/disable indexing logs automatically after fetching logs (default = enabled).
log-filter-status {enable disable}	Enable/Disable log-filter (default = disabled).
log-filter-logic {and or}	Set the logic for the log filters (default = or).
name <string>	The name of log-fetch client profile.
password <passwd>	The log-fetch server password.
peer-cert-cn <string>	Certificate common name for the log-fetch server. Note: Null or '-' means no certificate CN for the log-fetch server. Multiple CNs are separated by commas. If there is comma in CN, it must follow an escape character.
secure-connection {enable disable}	Enable/disable protecting log-fetch connection with TLS/SSL (default = enabled).
server-adom <string>	Log-fetch server side's adom name.
server-ip <ip>	The log fetch server IPv4 address.
start-time <hh:mm> <yyyy/mm/dd>	Set the start date and time of the data-range. The start date should be earlier than the end date.
sync-adom-config {enable disable}	Enable/disable ADOM configuration synchronization.
user <string>	The log-fetch server username.
Variables for config device-filter subcommand:	
<id>	Add or edit a device filter.
adom <string>	Enter the ADOM name.
device <device>	Enter the device name or serial number.
vdom <string>	Enter the VDOM, if required.
Variables for config log-filter subcommand:	
<id>	The log filter ID.
field <string>	Enter the field name.

Variable	Description
oper {= != < > <= >= contain not-contain match}	Set the filter operator.
value <string>	Enter the field filter operand or free-text matching expression.

log-fetch server-setting

Use this command to configure the fetching server settings.

Syntax

```
config system log-fetch server-setting
    set max-conn-per-session <integer>
    set max-sessions <integer>
    set user <string>
end
```

Variable	Description
max-conn-per-session <integer>	The maximum number of concurrent file download connections per session (default = 3).
max-sessions <integer>	The maximum number of concurrent fetch sessions (default = 1).
session-timeout <integer>	Set the fetch session timeout period, in minutes (default = 10). This option is only available in server mode.

log-forward

Use the following commands to configure log forwarding.

Syntax

```
config system log-forward
    edit <id>
        set mode {aggregation | disable | forwarding}
        set agg-archive-types {Web_Archive Secure_Web_Archive Email_Archive File_Transfer_Archive IM_Archive MMS_Archive AV_Quarantine IPS_Packets}
        set agg-data-end-time <hh:mm yyyy/mm/dd>
        set agg-data-start-time <hh:mm> <yyyy/mm/dd>
        set agg-logtypes {none app-ctrl attack content dlp emailfilter event generic history traffic virus webfilter netscan fct-event fct-traffic fct-netscan waf gtp dns ssh}
        set agg-password <passwd>
        set agg-schedule {daily | on-demand}
        set agg-time <integer>
        set agg-user <string>
```

```

set fwd-archives {enable | disable}
set fwd-archive-types {Web_Archive Email_Archive IM_Archive File_Transfer_Archive
    MMS_Archive AV_Quarantine IPS_Packets EDISC_Archive}
set fwd-compression {enable | disable}
set fwd-facility {alert | audit | auth | authpriv | clock | cron | daemon | ftp |
    kernel | local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7
    | lpr | mail | news | ntp | syslog | user | uucp}
set fwd-ha-bind-vip {enable | disable}
set fwd-log-source-ip {local_ip | original_ip}
set fwd-max-delay {1min | 5min | realtime}
set fwd-reliable {enable | disable}
set fwd-secure {enable | disable}
set fwd-server-type {cef | fortianalyzer | syslog}
set fwd-syslog-format {fgt | rfc-5424}
set log-field-exclusion-status {enable | disable}
set log-filter-logic {and | or}
set log-filter-status {enable | disable}
set log-masking-custom-priority disable
set log-masking-fields {domain dstip dstname email message srcip srcmac srcname
    user}
set log-masking-key <passwd>
set log-masking-status {enable | disable}
set pcapurl-enrich
set pcapurl-domain-ip
set peer-cert-cn <string>
set proxy-service {enable | disable}
set proxy-service-priority <integer>
set server-addr <string>
set server-device <string>
set server-name <string>
set server-port <integer>
set signature <integer>
set sync-metadata [sf-topology | interface-role | device | endusr-avatar]
config device-filter
    edit <id>
        set action {include}
        set adom <string>
        set device <string>
    end
config log-field-exclusion
    edit <id>
        set dev-type {FortiGate | FortiMail | FortiManager | FortiAnalyzer | FortiWeb
            | FortiCache | FortiSandbox | FortiDDoS | Syslog}
        set field-list <string>
        set log-type {app-ctrl | attack | content | dlp | emailfilter | event |
            generic | history | traffic | virus | voip | webfilter | netscan | waf |
            gtp | dns | ssh | ANY-TYPE}
    end
config log-filter
    edit <id>
        set field {type | logid | level | devid | vd | srcip | srcintf | srcport |
            dstip | dstintf | dstport | user | group | free-text }
        set oper {= | != | < | > | <= | >= | contain | not-contain | match}
        set value {traffic | event | utm}
    end
config log-masking-custom
    edit <id>
        set field-name <string>

```

```

        set field-type {email | ip | mac | string | unknown}
    end
end

```

Variable	Description
<id>	Enter the log aggregation ID that you want to edit.
mode {aggregation disable forwarding}	Log aggregation mode: <ul style="list-style-type: none"> aggregation: Aggregate logs to FortiAnalyzer disable: Do not forward or aggregate logs (default) forwarding: Forward logs to the FortiAnalyzer
agg-archive-types {Web_Archive Secure_Web_Archive Email_Archive File_Transfer_Archive IM_Archive MMS_Archive AV_Quarantine IPS_Packets}	Archive type (default = all options). This command is only available when the mode is set to aggregation.
agg-data-end-time <hh:mm yyyy/mm/dd>	Enter the end date and time of the data-range <hh:mm yyyy/mm/dd>. This command is only available when the mode is set to aggregation. Note: Use colon to connect hour and minute values. Use slash to connect year, month, and day values.
agg-data-start-time <hh:mm> <yyyy/mm/dd>	Enter the start date and time of the data-range <hh:mm yyyy/mm/dd>. This command is only available when the mode is set to aggregation. Note: Use colon to connect hour and minute values. Use slash to connect year, month, and day values.
agg-logtypes {none app-ctrl attack content dlp emailfilter event generic history traffic virus webfilter netscan fct-event fct-traffic fct-netscan waf gtp dns ssh}	Log type (default = all options). This command is only available when the mode is set to aggregation.
agg-password <passwd>	Log aggregation access password for server. This command is only available when the mode is set to aggregation.
agg-schedule {daily on-demand}	Schedule log aggregation mode (default = daily): <ul style="list-style-type: none"> daily: Run daily log aggregation. on-demand: Run log aggregation on demand. This command is only available when the mode is set to aggregation.
agg-time <integer>	Daily at the selected time (0 - 23, default = 0). This command is only available when the mode is set to aggregation.
agg-user <string>	Log aggregation access user name for server. This command is only available when the mode is set to aggregation.
fwd-archives {enable disable}	Enable/disable forwarding archives (default = enable). This command is only available when the mode is set to forwarding.

Variable	Description
<code>fwd-archive-types {Web_Archive Email_Archive IM_Archive File_ Transfer_Archive MMS_Archive AV_Quarantine IPS_Packets EDISC_Archive}</code>	Set the forwarding archive types (default = all options). This command is only available when the mode is set to <code>forwarding</code> .
<code>fwd-compression {enable disable}</code>	Enable/disable compression for better bandwidth efficiency (default = disable). This command is only available when the mode is set to <code>forwarding</code> .
<code>fwd-facility {alert audit auth authpriv clock cron daemon ftp kernel local0 local1 local2 local3 local4 local5 local6 local7 lpr mail news ntp syslog user uucp}</code>	<p>Facility for remote syslog (default = local7).</p> <ul style="list-style-type: none"> <code>alert</code>: Log alert <code>audit</code>: Log audit <code>auth</code>: Security/authorization messages <code>authpriv</code>: Security/authorization messages (private) <code>clock</code>: Clock daemon <code>cron</code>: Clock daemon <code>daemon</code>: System daemons <code>ftp</code>: FTP daemon <code>kernel</code>: Kernel messages <code>local0, local1, local2, local3, local4, local5, local6, local7</code>: Reserved for local use <code>lpr</code>: Line printer subsystem <code>mail</code>: Mail system <code>news</code>: Network news subsystem <code>ntp</code>: NTP daemon <code>syslog</code>: Messages generated internally by <code>syslogd</code> <code>user</code>: Random user level messages <code>uucp</code>: Network news subsystem <p>This command is only available when the mode is set to <code>forwarding</code>.</p>
<code>fwd-ha-bind-vip {enable disable}</code>	Always use VIP as the forwarding port when HA is enabled (default = enable). This command is only available when the mode is set to <code>forwarding</code> .
<code>fwd-log-source-ip {local_ip original_ip}</code>	The logs source IP address (default = local_ip). This command is only available when the mode is set to <code>forwarding</code> .
<code>fwd-max-delay {1min 5min realtime}</code>	<p>The maximum delay for near realtime log forwarding.</p> <ul style="list-style-type: none"> <code>1min</code>: Near realtime forwarding with up to one minute delay. <code>5min</code>: Near realtime forwarding with up to five minutes delay (default). <code>realtime</code>: Realtime forwarding, no delay. <p>This command is only available when the mode is set to <code>forwarding</code>.</p>
<code>fwd-reliable {enable disable}</code>	Enable/disable reliable logging (default = disable). This command is only available when the mode is set to <code>forwarding</code> .
<code>fwd-secure {enable disable}</code>	Enable/disable TLS/SSL secured reliable logging (default = disable). This command is only available when the mode is set to <code>forwarding</code> , <code>fwd-reliable</code> is enabled, and <code>fwd-server-type</code> is set to <code>cef</code> or <code>syslog</code> .

Variable	Description
<code>fwd-server-type {cef fortianalyzer syslog}</code>	Forwarding all logs to a CEF (Common Event Format) server, syslog server, or the FortiAnalyzer device (default = fortianalyzer). This command is only available when the mode is set to <code>forwarding</code> .
<code>fwd-syslog-format {fgt rfc-5424}</code>	Forwarding format for syslog. <ul style="list-style-type: none"> <code>fgt</code>: FortiGate syslog format (default). <code>rfc-5424</code>: rfc-5424 syslog format. This command is only available when the mode is set to <code>forwarding</code> and <code>fwd-server-type</code> is <code>syslog</code> .
<code>log-field-exclusion-status {enable disable}</code>	Enable/disable log field exclusion list (default = disable). This command is only available when the mode is set to <code>forwarding</code> and <code>fwd-server-type</code> is set to <code>cef</code> or <code>syslog</code> .
<code>log-filter-logic {and or}</code>	Logic operator used to connect filters (default = or). This command is only available when <code>log-filter-status</code> is enabled.
<code>log-filter-status {enable disable}</code>	Enable/disable log filtering (default = disable). This command is only available when the mode is set to <code>forwarding</code> .
<code>log-masking-custom-priority disable</code>	Disable custom field search priority. This command is only available when the mode is set to <code>forwarding</code> and <code>log-masking-status</code> is enabled.
<code>log-masking-fields {domain dstip dstname email message srcip srcmac srcname user}</code>	Log field masking fields . This command is only available when the mode is set to <code>forwarding</code> and <code>log-masking-status</code> is enabled.
<code>log-masking-key <passwd></code>	Enter the log field masking key. This command is only available when the mode is set to <code>forwarding</code> and <code>log-masking-status</code> is enabled.
<code>log-masking-status {enable disable}</code>	Enable/disable log field masking (default = disable). This command is only available when the mode is set to <code>forwarding</code> .
<code>pcapurl-enrich</code>	
<code>pcapurl-domain-ip</code>	
<code>peer-cert-cn <string></code>	
<code>proxy-service {enable disable}</code>	Enable/disable proxy service under collector mode (default = enable). This command is only available when the mode is set to <code>forwarding</code> .
<code>proxy-service-priority <integer></code>	Proxy service priority from 1 (lowest) to 20 (highest) (default = 10). This command is only available when the mode is set to <code>forwarding</code> .
<code>server-addr <string></code>	Remote server address.
<code>server-device <id></code>	Log aggregation server device ID.
<code>server-name <string></code>	Log aggregation server name.

Variable	Description
server-port <integer>	Enter the server listen port (1 - 65535, default = 514). This command is only available when the mode is set to <code>forwarding</code> .
signature <integer>	This field is auto-generated and should not be set.
sync-metadata [sf-topology interface-role device endusr-avatar]	<p>Synchronizing metadata types:</p> <ul style="list-style-type: none"> • <code>sf-topology</code>: Security Fabric topology • <code>interface-role</code>: Interface Role • <code>device</code>: Device information • <code>endusr-avatar</code>: End-user avatar <p>This command is only available when the mode is set to <code>forwarding</code>.</p>
Variables for <code>config device-filter</code> subcommand:	
<id>	Enter the device filter ID or enter a number to create a new entry.
action {include}	Include the specified device.
adom <string>	<p>Enter the ADOM name from the following:</p> <ul style="list-style-type: none"> • <code>FortiAnalyzer</code> • <code>FortiAuthenticator</code> • <code>FortiCache</code> • <code>FortiCarrier</code> • <code>FortiClient</code> • <code>FortiDDoS</code> • <code>FortiDeceptor</code> • <code>FortiFirewall</code> • <code>FortiFirewallCarrier</code> • <code>FortiMail</code> • <code>FortiManager</code> • <code>FortiProxy</code> • <code>FortiSandbox</code> • <code>FortiWeb</code> • <code>Syslog</code> • <code>Unmanaged_Devices</code> • <code>root</code> <p>Alternatively, enter (null) for all ADOM(s) or a wildcard expression matching ADOM(s).</p>
device <string>	Device ID of log client device, or a wildcard expression matching log client device (s).
Variables for <code>config log-field-exclusions</code> subcommand:	
This command is only available when the mode is set to <code>forwarding</code> and <code>log-field-exclusions-status</code> is set to <code>enable</code> .	
<id>	Enter a device filter ID or enter a number to create a new entry.

Variable	Description
dev-type {FortiGate FortiMail FortiManager FortiAnalyzer FortiWeb FortiCache FortiSandbox FortiDDoS Syslog}	The device type (default = FortiGate).
field-list <string>	The field type. Enter a comma separated list from the available fields.
log-type {app-ctrl attack content dlp emailfilter event generic history traffic virus voip webfilter netscan waf gtp dns ssh ANY-TYPE}	The log type (default = traffic).
Variables for <code>config log-filter</code> subcommand: This command is only available when the mode is set to forwarding and log-field-status is set to enable.	
<id>	Enter the log filter ID or enter a number to create a new entry.
field {type logid level devid vd srcip srcintf srcport dstip dstintf dstport user group free-text}	Field name (default = type).
oper {= != < > <= >= contain not-contain match}	Field filter operator (default = =).
value {traffic event utm}	Field filter operand or free-text matching expression. This variable uses the glibc regex library for values with operators (~,!~), using the POSIX standard. Filter string syntax is parsed by FortiAnalyzer, escape characters must be use when needed, and both upper and lower case characters are supported. For example: "a ~ \"regexp\" and (c==d OR e==f) "
Variables for <code>log-masking-custom</code> subcommand: This command is only available when the mode is set to forwarding and log-masking-status is enabled.	
<id>	Enter the log field masking ID or enter a number to create a new entry.
field-name <string>	Field name.
field-type {email ip mac string unknown}	Field type (default = unknown).

log-forward-service

Use the following commands to configure log aggregation service.



This command is only available on FortiAnalyzer models 1000E and above. It is also available on all supported FortiAnalyzer-VM.

For a list of supported models in v7.0.10, see the [FortiAnalyzer 7.0.10 Release Notes](#).

Syntax

```
config system log-forward-service
  set accept-aggregation {enable | disable}
  set aggregation-disk-quota <integer>
end
```

Variable	Description
accept-aggregation {enable disable}	Enable/disable accept log aggregation option (default = disable).
aggregation-disk-quota <integer>	Aggregated device disk quota on the server, in megabytes (default = 2000).

mail

Use this command to configure mail servers on your FortiAnalyzer unit.

Syntax

```
config system mail
  edit <id>
    set auth {enable | disable}
    set auth-type {certificate | psk}
    set from <string>
    set local-cert {Fortinet_Local | Fortinet_Local2}
    set passwd <passwd>
    set port <integer>
    set secure-option {default | none | smtps | starttls}
    set server <string>
    set user <string>
  end
```

Variable	Description
<id>	Enter the mail service ID of the entry you would like to edit or type a new name to create an entry (character limit = 63).
auth {enable disable}	Enable/disable authentication (default = disable).
auth-type {certificate psk}	Select the SMTP authentication type (default = psk): <ul style="list-style-type: none"> certificate: Use local certificate to authenticate. psk: Use username and password to authenticate.

Variable	Description
from <string>	Set the SMTP default username for sending.
local-cert {Fortinet_Local Fortinet_Local2}	Choose from the two available local certificates. This variable is available only when the <code>auth-type</code> is <code>certificate</code> .
passwd <passwd>	Enter the SMTP account password value (character limit = 63). This variable is available only when the <code>auth-type</code> is <code>psk</code> .
port <integer>	Enter the SMTP server port (1 - 65535, default = 25).
secure-option {default none smtps starttls}	Select the communication secure option: <ul style="list-style-type: none"> <code>default</code>: Try STARTTLS, proceed as plain text communication otherwise (default). <code>none</code>: Communication will be in plain text format. <code>smtps</code>: Communication will be protected by SMTPS. <code>starttls</code>: Communication will be protected by STARTTLS.
server <string>	Enter the SMTP server name.
user <string>	Enter the SMTP account user name. This variable is available only when the <code>auth-type</code> is <code>psk</code> .

metadata

Use this command to add additional information fields to the administrator accounts of your FortiAnalyzer unit.



This command creates the metadata fields. Use `config system admin user` to add data to the metadata fields.

Syntax

```
config system metadata admins
edit <fieldname>
set fieldlength {20 | 255 | 50}
set importance {optional | required}
set status {enable | disable}
end
```

Variable	Description
<fieldname>	Enter the name of the field.
fieldlength {20 255 50}	Select the maximum number of characters allowed in this field (default = 50).
importance {optional required}	Select if this field is required or optional when entering standard information (default = required).

Variable	Description
status {enable disable}	Enable/disable the metadata (default = enabled).

ntp

Use this command to configure automatic time setting using a network time protocol (NTP) server.

Syntax

```
config system ntp
  set status {enable | disable}
  config ntpserver
    edit <id>
      set ntpv3 {enable | disable}
      set authentication {enable | disable}
      set key <passwd>
      set key-id <integer>
      set server <string>
      set minpoll <integer>
      set maxpoll <integer>
    end
  end
```

Variable	Description
status {enable disable}	Enable/disable NTP time setting (default = enable).
Variables for <code>config ntpserver</code> subcommand:	
<id>	Time server ID.
ntpv3 {enable disable}	Enable/disable NTPv3 (default = disable).
authentication {enable disable}	Enable/disable MD5 authentication (default = disable).
key <passwd>	The authentication key (character limit = 63).
key-id <integer>	The key ID for authentication (default = 0).
server <string>	Enter the IPv4 or IPv6 address, or fully qualified domain name of the NTP server (default = ntpl.fortinet.com).
minpoll <integer>	Minimum poll interval in seconds as power of 2 (e.g. 6 means 64 seconds, default = 6).
maxpoll <integer>	Maximum poll interval in seconds as power of 2 (e.g. 6 means 64 seconds, default = 10).

password-policy

Use this command to configure access password policies.

Syntax

```
config system password-policy
  set status {enable | disable}
  set minimum-length <integer>
  set must-contain {lower-case-letter non-alphanumeric number upper-case-letter}
  set change-4-characters {enable | disable}
  set expire <integer>
end
```

Variable	Description
status {enable disable}	Enable/disable the password policy (default = disable).
minimum-length <integer>	Set the password's minimum length (8 - 256, default = 8).
must-contain {lower-case-letter non-alphanumeric number upper-case-letter}	Characters that a password must contain. <ul style="list-style-type: none">lower-case-letter: the password must contain at least one lower case letternon-alphanumeric: the password must contain at least one non-alphanumeric charactersnumber: the password must contain at least one numberupper-case-letter: the password must contain at least one upper case letter.
change-4-characters {enable disable}	Enable/disable changing at least 4 characters for a new password (default = disable).
expire <integer>	Set the number of days after which admin users' passwords will expire (0 - 3650, 0 = never, default = 0).

report

Use the following command to configure report related settings.

report auto-cache

Use this command to view or configure report auto-cache settings.

Syntax

```
config system report auto-cache
  set aggressive-schedule {enable | disable}
```

```

set order {latest-first | oldest-first}
set sche-rpt-only {enable | disable}
set status {enable | disable}
end

```

Variable	Description
aggressive-schedule {enable disable}	Enable/disable auto-cache on schedule reports aggressively (default = disable).
order {latest-first oldest-first}	The order of which SQL log table is processed first: <ul style="list-style-type: none"> latest-first: The newest SQL log table is processed first. oldest-first: The oldest SQL log table is processed first (default).
sche-rpt-only {enable disable}	Enable/disable auto-cache on scheduled reports only (default = disable).
status {enable disable}	Enable/disable the SQL report auto-cache (default = enable).

report est-browse-time

Use this command to view or configure report settings.

Syntax

```

config system report est-browse-time
set max-read-time <integer>
set status {enable | disable}
end

```

Variable	Description
max-read-time <integer>	Set the read time threshold for each page view (1 - 3600, default = 180).
status {enable disable}	Enable/disable estimating browse time (default = enable).

report group

Use these commands to configure report groups.

Syntax

```

config system report group
edit <group-id>
set adom <adom-name>
set case-insensitive {enable | disable}
set report-like <string>
config chart-alternative
edit <chart-name>
set chart-replace <string>
end
config group-by

```

```

        edit <var-name>
            set var-expression <string>
            set var-type {enum | integer | ip | string}
        end
    end
end

```

Variable	Description
<group-id>	The identification number of the group to be edited or created.
adom <adom-name>	The ADOM that contains the report group.
case-insensitive {enable disable}	Enable/disable case sensitivity (default = enable).
report-like <string>	Report pattern
Variables for config chart-alternative subcommand:	
<chart-name>	The chart name.
chart-replace <string>	Chart replacement.
Variable for config group-by subcommand:	
<var-name>	The variable name.
var-expression <string>	Variable expression.
var-type {enum integer ip string}	Variable type (default = string).

report setting

Use these commands to view or configure report settings.

Syntax

```

config system report setting
    set aggregate-report {enable | disable}
    set capwap-port <integer>
    set capwap-service <string>
    set exclude-capwap {by-port | by-service | disable}
    set hcache-lossless {enable | disable}
    set ldap-cache-timeout <integer>
    set max-rpt-pdf-rows <integer>
    set max-table-rows <integer>
    set report-priority {auto | high | low}
    set template-auto-install {default}
    set week-start {mon | sun}
end

```

Variable	Description
aggregate-report {enable disable}	Enable/disable including a group report along with the per-device reports (default = disable).
capwap-port <integer>	Exclude capwap traffic by port (default = 5246).
capwap-service <string>	Exclude capwap traffic by service.
exclude-capwap {by-port by-service disable}	Exclude capwap traffic (default = by-port).
hcache-lossless {enable disable}	Enable/disable ready-with-loss hcaches (default = disable).
ldap-cache-timeout <integer>	Set the LDAP cache timeout in minutes (0 = do not use cache, default = 60).
max-rpt-pdf-rows <integer>	Set the maximum number of rows that can be generated in a single pdf (10000 - 1000000, default = 100000).
max-table-rows <integer>	Set the maximum number of rows that can be generated in a single table (10000 - 10000000, default = 1000000).
report-priority {auto high low}	Set the Priority of the SQL report (default = auto).
template-auto-install {default}	Set the language used for new ADOMs (default = default).
week-start {mon sun}	Set the day that the week starts on, either <code>sun</code> (Sunday) or <code>mon</code> (Monday) (default = sun).

route

Use this command to view or configure static routing table entries on your FortiAnalyzer unit.

Syntax

```
config system route
  edit <seq_int>
    set device <port>
    set dst <dst_ipv4mask>
    set gateway <gateway_ipv4_address>
  end
```

Variable	Description
<seq_int>	Enter an unused routing sequence number to create a new route. Enter an existing route number to edit that route.
device <port>	Enter the port (interface) used for this route.
dst <dst_ipv4mask>	Enter the IPv4 address and mask for the destination network.
gateway <gateway_ipv4_address>	Enter the default gateway IPv4 address for this network.

route6

Use this command to view or configure static IPv6 routing table entries on your FortiAnalyzer unit.

Syntax

```
config system route6
  edit <seq_int>
    set device <string>
    set dst <ipv6_prefix>
    set gateway <ipv6_address>
  end
```

Variable	Description
<seq_int>	Enter an unused routing sequence number to create a new route. Enter an existing route number to edit that route.
device <string>	Enter the port (interface) used for this route.
dst <ipv6_prefix>	Enter the IPv4 address and mask for the destination network.
gateway <ipv6_address>	Enter the default gateway IPv6 address for this network.

saml

Use this command to configure global settings for SAML authentication.

Syntax

```
config system saml
  set acs-url
  set cert <certificate>
  set default-profile <string>
  set entity-id <string>
  set forticloud-sso {enable | disable}
  set idp-cert <string>
  set idp-entity-id <string>
  set idp-single-logout-url <string>
  set idp-single-sign-on-url <string>
  set login-auto-redirect {enable | disable}
  set role {FAB-SP | IDP | SP}
  set server-address <string>
  set sls-url
  set status {enable | disable}
  set user-auto-create {enable | disable}
  config service-providers
    edit <name>
      set idp-entity-id <string>
      set idp-single-logout-url <string>
```

```

        set idp-single-sign-on-url <string>
        set prefix <string>
        set sp-cert <string>
        set sp-entity-id <string>
        set sp-single-logout-url <string>
        set sp-single-sign-on-url <string>
    next
end
config fabric-idp
    edit <device-id>
        set idp-cert <string>
        set idp-entity-id <string>
        set idp-single-logout-url <string>
        set idp-single-sign-on-url <string>
        set idp-status {enable | disable}
    next
end
end

```

Variable	Description
acs-url	
cert <certificate>	The certificate name.
default-profile <string>	The default profile (default = Restricted_User).
entity-id <string>	The entity ID.
forticloud-sso {enable disable}	Enable/disable FortiCloud SSO (default = disable).
idp-cert <string>	The IDP certificate name.
idp-entity-id <string>	The IDP entity ID.
idp-single-logout-url <string>	The IDP single logout URL.
idp-single-sign-on-url <string>	The IDP single sign-on URL.
login-auto-redirect {enable disable}	Enable/disable automatic redirect to the IDP login page (default = disable).
role {FAB-SP IDP SP}	The SAML role: <ul style="list-style-type: none"> FAB-SP: Fabric service provider IDP: Identity provider SP: Service provider (default)
server-address <string>	The server address.
sls-url	
status {enable disable}	Enable/disable SAML authentication (default = disable).
user-auto-create {enable disable}	Enable/disable automatic user creation (default = disable).
Variables for config service-providers subcommand: This command is only available when role is IDP.	

Variable	Description
<name>	Service provide name.
idp-entity-id <string>	The IDP entity ID.
idp-single-logout-url <string>	The IDP single logout URL.
idp-single-sign-on-url <string>	The IDP single sign-on URL.
prefix <string>	The prefix. Can contain only letters and numbers.
sp-cert <string>	The SP certificate name.
sp-entity-id <string>	The SP entity ID.
sp-single-logout-url <string>	The SP single sign-on URL.
sp-single-sign-on-url <string>	The SP single logout URL.
Variables for <code>config fabric-idp</code> subcommand:	
This command is only available when <code>role</code> is <code>FAB-SP</code> .	
<device-id>	Device ID.
idp-cert <string>	The IDP certificate name.
idp-entity-id <string>	The IDP entity ID.
idp-single-logout-url <string>	The IDP single logout URL.
idp-single-sign-on-url <string>	The IDP single sign-on URL.
idp-status {enable disable}	Enable/disable SAML authentication (default = disable).

To view the service provider IdP information, use the following commands:

```
config system saml
  config service-providers
    edit <name>
      get
```

Output:

```
name : name prefix : y9jr06vq0k sp-cert : (null) sp-entity-id :
http://https://172.27.2.225//metadata/ sp-single-sign-on-url:
https://https://172.27.2.225//saml/?acs sp-single-logout-url:
https://https://172.27.2.225//saml/?sls idp-entity-id : http://172.27.2.225/saml-
idp/y9jr06vq0k/metadata/ idp-single-sign-on-url: https://172.27.2.225/saml-
idp/y9jr06vq0k/login/ idp-single-logout-url: https://172.27.2.225/saml-
idp/y9jr06vq0k/logout/
```

sniffer

Configure packet sniffing.

Syntax

```
config system sniffer
  edit <id>
    set host <string>
    set interface <interface>
    set ipv6 {enable | disable}
    set max-packet-count <integer>
    set non-ip {enable | disable}
    set port <string>
    set protocol <string>
    set vlan <string>
  next
end
```

Variable	Description
<id>	Sniffer ID.
host <string>	IP addresses of the hosts to filter for in sniffer traffic. Multiple individual IP addresses and ranges of addresses can be entered.
interface <interface>	The interface to sniff.
ipv6 {enable disable}	Enable/disable sniffing IPv6 packets.
max-packet-count <integer>	The maximum packet count (1 - 1000000, default - 4000).
non-ip {enable disable}	Enable/disable sniffing non-IP packets.
port <string>	The ports to sniff. Individual ports or port ranges can be entered.
protocol <string>	Integer value for the protocol type as defined by IANA (0 - 255).
vlan <string>	The VLANs to sniff.

snmp

Use the following commands to configure SNMP related settings.

snmp community

Use this command to configure SNMP communities on your FortiAnalyzer unit.

You add SNMP communities so that SNMP managers, typically applications running on computers to monitor SNMP status information, can connect to the FortiAnalyzer unit (the SNMP agent) to view system information and receive SNMP traps. SNMP traps are triggered when system events happen such as when there is a system restart, or when the log disk is almost full.

You can add up to three SNMP communities, and each community can have a different configuration for SNMP queries and traps. Each community can be configured to monitor the FortiAnalyzer unit for a different set of events.

Hosts are the SNMP managers that make up this SNMP community. Host information includes the IPv4 address and interface that connects it to the FortiAnalyzer unit.

For more information on SNMP traps and variables, see the [Fortinet Document Library](#).



Part of configuring an SNMP manager is to list it as a host in a community on the FortiAnalyzer unit that it will be monitoring. Otherwise that SNMP manager will not receive any traps or events from the FortiAnalyzer unit, and will be unable to query the FortiAnalyzer unit as well.

Syntax

```
config system snmp community
  edit <index_number>
    set events <events_list>
    set name <community_name>
    set query-vl-port <integer>
    set query-vl-status {enable | disable}
    set query-v2c-port <integer>
    set query-v2c-status {enable | disable}
    set status {enable | disable}
    set trap-vl-rport <integer>
    set trap-vl-status {enable | disable}
    set trap-v2c-rport <integer>
    set trap-v2c-status {enable | disable}
  config hosts
    edit <host_number>
      set interface <interface_name>
      set ip <ipv4_address>
    end
  config hosts6
    edit <host_number>
      set interface <interface_name>
      set ip <ipv6_address>
    end
  end
end
```

Variable	Description
<index_number>	Enter the index number of the community in the SNMP communities table. Enter an unused index number to create a new SNMP community.
events <events_list>	<p>Enable the events for which the FortiManager unit should send traps to the SNMP managers in this community (default = All events enabled). The <code>raid_changed</code> event is only available for devices that support RAID.</p> <ul style="list-style-type: none"> <code>cpu-high-exclude-nice</code>: CPU usage exclude NICE threshold. <code>cpu_high</code>: CPU usage too high. <code>disk_low</code>: Disk usage too high. <code>ha_switch</code>: HA switch. <code>intf_ip_chg</code>: Interface IP address changed. <code>lic-dev-quota</code>: High licensed device quota detected. <code>lic-gbday</code>: High licensed log GB/day detected.

Variable	Description
	<ul style="list-style-type: none"> • <code>log-alert</code>: Log base alert message. • <code>log-data-rate</code>: High incoming log data rate detected. • <code>log-rate</code>: High incoming log rate detected. • <code>mem_low</code>: Available memory is low. • <code>raid_changed</code>: RAID status changed. • <code>sys_reboot</code>: System reboot.
<code>name <community_name></code>	<p>Enter the name of the SNMP community. Names can be used to distinguish between the roles of the hosts in the groups.</p> <p>For example the Logging and Reporting group would be interested in the <code>disk_low</code> events, but likely not the other events.</p> <p>The name is included in SNMPv2c trap packets to the SNMP manager, and is also present in query packets from, the SNMP manager.</p>
<code>query-v1-port <integer></code>	Enter the SNMPv1 query port number used when SNMP managers query the FortiManager unit (1 - 65535, default = 161).
<code>query-v1-status {enable disable}</code>	Enable/disable SNMPv1 queries for this SNMP community (default = enable).
<code>query-v2c-port <integer></code>	Enter the SNMP v2c query port number used when SNMP managers query the FortiManager unit. SNMP v2c queries will include the name of the community (1 - 65535, default = 161).
<code>query-v2c-status {enable disable}</code>	Enable/disable SNMPv2c queries for this SNMP community (default = enable).
<code>status {enable disable}</code>	Enable/disable this SNMP community (default = enable).
<code>trap-v1-rport <integer></code>	Enter the SNMPv1 remote port number used for sending traps to the SNMP managers (1 - 65535, default = 162).
<code>trap-v1-status {enable disable}</code>	Enable/disable SNMPv1 traps for this SNMP community (default = enable).
<code>trap-v2c-rport <integer></code>	Enter the SNMPv2c remote port number used for sending traps to the SNMP managers (1 - 65535, default = 162).
<code>trap-v2c-status {enable disable}</code>	Enable/disable SNMPv2c traps for this SNMP community. SNMP v2c traps sent out to SNMP managers include the community name (default = enable).
Variables for <code>config hosts</code> subcommand:	
<code><host_number></code>	Enter the index number of the host in the table. Enter an unused index number to create a new host.
<code>interface <interface_name></code>	Enter the name of the FortiAnalyzer unit that connects to the SNMP manager (default = any).
<code>ip <ipv4_address></code>	Enter the IPv4 address of the SNMP manager.
Variables for <code>config hosts6</code> subcommand:	

Variable	Description
<host_number>	Enter the index number of the host in the table. Enter an unused index number to create a new host.
interface <interface_name>	Enter the name of the FortiAnalyzer unit that connects to the SNMP manager (default = any).
ip <ipv6_address>	Enter the IPv6 address of the SNMP manager.

Example

This example shows how to add a new SNMP community named `SNMP_Com1`. The default configuration can be used in most cases with only a few modifications. In the example below the community is added, given a name, and then because this community is for an SNMP manager that is SNMP v1 compatible, all v2c functionality is disabled. After the community is configured the SNMP manager, or host, is added. The SNMP manager IPv4 address is 192.168.20.34 and it connects to the FortiAnalyzer unit internal interface.

```
config system snmp community
  edit 1
    set name SNMP_Com1
    set query-v2c-status disable
    set trap-v2c-status disable
    config hosts
      edit 1
        set interface internal
        set ip 192.168.10.34
      end
    end
end
```

snmp sysinfo

Use this command to enable the FortiAnalyzer SNMP agent and to enter basic system information used by the SNMP agent. Enter information about the FortiAnalyzer unit to identify it. When your SNMP manager receives traps from the FortiAnalyzer unit, you will know which unit sent the information. Some SNMP traps indicate high CPU usage, log full, or low memory.

For more information on SNMP traps and variables, see the [Fortinet Document Library](#).

Syntax

```
config system snmp sysinfo
  set contact-info <string>
  set description <description>
  set engine-id <string>
  set fortianalyzer-legacy-sysoid <string>
  set location <location>
  set status {enable | disable}
  set trap-cpu-high-exclude-nice-threshold <percentage>
  set trap-high-cpu-threshold <percentage>
  set trap-low-memory-threshold <percentage>
end
```

Variable	Description
contact-info <string>	Add the contact information for the person responsible for this FortiAnalyzer unit (character limit = 255).
description <description>	Add a name or description of the FortiManager unit (character limit = 255).
engine-id <string>	Local SNMP engine ID string (character limit = 24).
fortianalyzer-legacy-sysoid <string>	Enable to switch back to legacy FortiAnalyzer sysObjectOID (default = disable)..
location <location>	Describe the physical location of the FortiAnalyzer unit (character limit = 255).
status {enable disable}	Enable/disable the FortiAnalyzer SNMP agent (default = disable).
trap-cpu-high-exclude-nice-threshold <percentage>	SNMP trap for CPU usage threshold (excluding NICE processes), in percent (default = 80).
trap-high-cpu-threshold <percentage>	SNMP trap for CPU usage threshold, in percent (default = 80).
trap-low-memory-threshold <percentage>	SNMP trap for memory usage threshold, in percent (default = 80).

Example

This example shows how to enable the FortiAnalyzer SNMP agent and add basic SNMP information.

```
config system snmp sysinfo
  set status enable
  set contact-info 'System Admin ext 245'
  set description 'Internal network unit'
  set location 'Server Room A121'
end
```

snmp user

Use this command to configure SNMPv3 users on your FortiAnalyzer unit. To use SNMPv3, you will first need to enable the FortiAnalyzer SNMP agent. For more information, see [snmp sysinfo](#). There should be a corresponding configuration on the SNMP server in order to query to or receive traps from FortiAnalyzer.

For more information on SNMP traps and variables, see the [Fortinet Document Library](#).

Syntax

```
config system snmp user
  edit <name>
    set auth-proto {md5 | sha}
    set auth-pwd <passwd>
    set events <events_list>
    set notify-hosts <ipv4_address>
    set notify-hosts6 <ipv6_address>
    set priv-protocol {aes | des}
```



```

    set priv-pwd <passwd>
    set queries {enable | disable}
    set query-port <integer>
    set security-level {auth-no-priv | auth-priv | no-auth-no-priv}
end
end

```

Variable	Description
<name>	Enter a SNMPv3 user name to add, edit, or delete.
auth-proto {md5 sha}	Authentication protocol. The security level must be set to <code>auth-no-priv</code> or <code>auth-priv</code> to use this variable: <ul style="list-style-type: none"> md5: HMAC-MD5-96 authentication protocol sha: HMAC-SHA-96 authentication protocol (default)
auth-pwd <passwd>	Password for the authentication protocol. The security level must be set to <code>auth-no-priv</code> or <code>auth-priv</code> to use this variable.
events <events_list>	Enable the events for which the FortiAnalyzer unit should send traps to the SNMPv3 managers in this community (default = All events enabled). The <code>raid_changed</code> event is only available for devices which support RAID. <ul style="list-style-type: none"> cpu-high-exclude-nice: CPU usage exclude nice threshold. cpu_high: The CPU usage is too high. disk_low: The log disk is getting close to being full. ha_switch: A new unit has become the primary HA. intf_ip_chg: An interface IP address has changed. lic-dev-quota: High licensed device quota detected. lic-gbday: High licensed log GB/Day detected. log-alert: Log base alert message. log-data-rate: High incoming log data rate detected. log-rate: High incoming log rate detected. mem_low: The available memory is low. raid_changed: RAID status changed. sys_reboot: The FortiAnalyzer unit has rebooted.
notify-hosts <ipv4_address>	Hosts to send notifications (traps) to.
notify-hosts6 <ipv6_address>	Hosts to send notifications (traps) to.
priv-proto {aes des}	Privacy (encryption) protocol. The security level must be set to <code>auth-no-priv</code> or <code>auth-priv</code> to use this variable: <ul style="list-style-type: none"> aes: CFB128-AES-128 symmetric encryption protocol (default) des: CBC-DES symmetric encryption protocol
priv-pwd <passwd>	Password for the privacy (encryption) protocol. The security level must be set to <code>auth-no-priv</code> or <code>auth-priv</code> to use this variable.
queries {enable disable}	Enable/disable queries for this user (default = enable)
query-port <integer>	SNMPv3 query port (1 - 65535, default = 161).
security-level {auth-no-priv auth-priv no-auth-no-priv}	Security level for message authentication and encryption: <ul style="list-style-type: none"> auth-no-priv: Message with authentication but no privacy (encryption).

Variable	Description
	<ul style="list-style-type: none">• <code>auth-priv</code>: Message with authentication and privacy (encryption).• <code>no-auth-no-priv</code>: Message with no authentication and no privacy (encryption) (default).

soc-fabric

Use this command to configure the SOC Fabric.

Syntax

```
config system soc-fabric
  set name <string>
  set port <integer>
  set psk <passwd>
  set role {member | supervisor}
  set secure-connection {enable | disable}
  set status {enable | disable}
  set supervisor <string>
end
```

Variable	Description
<code><name></code>	Enter the Fabric name.
<code>port <integer></code>	Set the communication port (1 - 65535, default = 6443).
<code>psk <passwd></code>	Enter the Fabric authentication password.
<code>role {member supervisor}</code>	Set the SOC Fabric role (default = member).
<code>secure-connection {enable disable}</code>	Enable/disable SSL/TLS (default = enable).
<code>status {enable disable}</code>	Enable/disable SOC Fabric (default = disable).
<code>supervisor <string></code>	Enter the IP/FQDN of the supervisor.

sql

Configure Structured Query Language (SQL) settings.

Syntax

```
config system sql
  set background-rebuild {enable | disable}
  set compress-table-min-age <integer>
```

```

set database-name <string>
set database-type <postgres>
set device-count-high {enable | disable}
set event-table-partition-time <integer>
set fct-table-partition-time <integer>
set logtype {none | app-ctrl | attack | content | dlp | emailfilter | event | generic
            | history | traffic | virus | voip | webfilter | netscan}
set password <passwd>
set prompt-sql-upgrade {enable | disable}
set rebuild-event {enable | disable}
set rebuild-event-start-time <hh:mm> <yyyy/mm/dd>
set server <string>
set start-time <hh>:<mm> <yyyy>/<mm>/<dd>
set status {disable | local}
set text-search-index {enable | disable}
set traffic-table-partition-time <integer>
set utm-table-partition-time <integer>
set username <string>
config custom-index
    edit <id>
        set case-sensitive {enable | disable}
        set device-type {FortiCache | FortiGate | FortiMail | FortiSandbox | FortiWeb}
        set index-field <Field-Name>
        set log-type <Log-Enter>
    next
end
config custom-skipidx
    edit <id>
        set device-type <device>
        set index-field <Field-Name>
        set log-type <Log-Enter>
    next
end
config ts-index-field
    edit <category>
        set <value> <string>
    next
end
end

```

Variable	Description
background-rebuild {enable disable}	Disable/enable rebuilding the SQL database in the background (default = enable).
compress-table-min-age <integer>	Minimum age in days for SQL tables to be compressed (0 - 10000, default = 7). Note: 0-day allows you to compress SQL tables with less than one-day of age.
database-name <string>	Remote SQL database name (character limit = 64).
database-type <postgres>	Database type (default = postgres).
device-count-high {enable disable}	Enable/disable a high device count (default = disable). You must set to enable if the count of registered devices is greater than 8000: <ul style="list-style-type: none"> disable: Set to disable if device count is less than 8000. enable: Set to enable if device count is equal to or greater than 8000.

Variable	Description
	Caution: Enabling or disabling this command will result in an SQL database rebuild. The time required to rebuild the database is dependent on the size of the database. Please plan a maintenance window to complete the database rebuild. This operation will also result in a device reboot.
event-table-partition-time <integer>	Maximum SQL database table partitioning time range for event logs, in minutes (3 - 1440, 0 = unlimited, default = 0).
fct-table-partition-time <integer>	Maximum SQL database table partitioning time range for FortiClient logs, in minutes (6 - 1440, 0 = unlimited, default = 360).
logtype {none app-ctrl attack content dlp emailfilter event generic history traffic virus voip webfilter netscan}	Log type.
password <passwd>	The password that the Fortinet unit will use to authenticate with the remote database.
prompt-sql-upgrade {enable disable}	Prompt to convert log database into SQL database at start time on GUI (default = enable).
rebuild-event {enable disable}	Enable/disable a rebuild event during SQL database rebuilding (default = enable).
rebuild-event-start-time <hh:mm> <yyyy/mm/dd>	The rebuild event starting date and time (default = 00:00 2000/01/01).
server <string>	Set the database ip or hostname.
start-time <hh>:<mm> <yyyy>/<mm>/<dd>	The date and time that logs will start to be inserted.
status {disable local}	SQL database status: <ul style="list-style-type: none"> <code>disable</code>: Disable SQL database. <code>local</code>: Enable local database (default).
text-search-index {enable disable}	Enable/disable the creation of a text search index (default = disable).
traffic-table-partition-time <integer>	Maximum SQL database table partitioning time range for traffic logs (1 - 1440, 0 = unlimited, default = 0).
utm-table-partition-time <integer>	Maximum SQL database table partitioning time range in minutes for UTM logs (1 - 1440, 0 = unlimited, default = 0).
username <string>	The user name that the unit will use to authenticate with the remote database (character limit = 64).
Variables for <code>config custom-index</code> subcommand:	
case-sensitive {enable disable}	Enable/disable case sensitivity.

Variable	Description
device-type {FortiAuthenticator FortiCache FortiClient FortiDDoS FortiGate FortiMail FortiManager FortiSandbox FortiWeb}	Set the device type (default = FortiGate).
index-field <Field-Name>	Enter a valid field name. Select one of the available field names. The available options for <code>index-field</code> is dependent on the <code>device-type</code> entry.
log-type <Log-Enter>	Enter the log type. The available options for <code>log-type</code> is dependent on the <code>device-type</code> entry.
Variables for <code>config custom-skipidx</code> subcommand: List of additional SQL skip index fields.	
device-type <device>	Set the device type (default = FortiGate).
index-field <Field-Name>	Enter a valid field name. Select one of the available field names. The available options depend on the <code>device-type</code> .
log-type <Log-Enter>	Enter the log type (default = traffic). The available options depend on the <code>device-type</code> .
Variables for <code>config ts-index-field</code> subcommand:	
<category>	Category of the text search index fields. The following is the list of categories and their default fields.
Category	Value
FGT-app-ctrl	user,group,srcip,dstip,dstport,service,app,action,hostname
FGT-attack	severity,srcip,dstip,action,user,attack
FGT-content	from,to,subject,action,srcip,dstip,hostname,status
FGT-dlp	user,srcip,service,action,filename
FGT-emailfilter	user,srcip,from,to,subject
FGT-event	subtype,ui,action,msg
FGT-traffic	user,srcip,dstip,service,app,utmaction
FGT-virus	service,srcip,dstip,action,filename,virus,user
FGT-voip	action,user,src,dst,from,to
FGT-webfilter	user,srcip,dstip,service,action,catdesc,hostname
FGT-netscan	user,dstip,vuln,severity,os
FGT-fct-event	(null)
FGT-fct-traffic	(null)

Variable	Description																										
	<table> <tr> <th>Category</th><th>Value</th></tr> <tr> <td>FGT-fct-netscan</td><td>(null)</td></tr> <tr> <td>FGT-waf</td><td>user,srcip,dstip,service,action</td></tr> <tr> <td>FGT-gtp</td><td>msisdn,from,to,status</td></tr> <tr> <td>FGT-dns</td><td>(null)</td></tr> <tr> <td>FGT-ssh</td><td>login,srcip,dstip,direction,action</td></tr> <tr> <td>FML-emailfilter</td><td>client_name,dst_ip,from,to,subject</td></tr> <tr> <td>FML-event</td><td>subtype,msg</td></tr> <tr> <td>FML-history</td><td>classifier,disposition,from,to,client_name,direction,domain,virus</td></tr> <tr> <td>FML-virus</td><td>src,msg,from,to</td></tr> <tr> <td>FWB-attack</td><td>http_host,http_url,src,dst,msg,action</td></tr> <tr> <td>FWB-event</td><td>ui,action,msg</td></tr> <tr> <td>FWB-traffic</td><td>src,dst,service,http_method,msg</td></tr> </table>	Category	Value	FGT-fct-netscan	(null)	FGT-waf	user,srcip,dstip,service,action	FGT-gtp	msisdn,from,to,status	FGT-dns	(null)	FGT-ssh	login,srcip,dstip,direction,action	FML-emailfilter	client_name,dst_ip,from,to,subject	FML-event	subtype,msg	FML-history	classifier,disposition,from,to,client_name,direction,domain,virus	FML-virus	src,msg,from,to	FWB-attack	http_host,http_url,src,dst,msg,action	FWB-event	ui,action,msg	FWB-traffic	src,dst,service,http_method,msg
Category	Value																										
FGT-fct-netscan	(null)																										
FGT-waf	user,srcip,dstip,service,action																										
FGT-gtp	msisdn,from,to,status																										
FGT-dns	(null)																										
FGT-ssh	login,srcip,dstip,direction,action																										
FML-emailfilter	client_name,dst_ip,from,to,subject																										
FML-event	subtype,msg																										
FML-history	classifier,disposition,from,to,client_name,direction,domain,virus																										
FML-virus	src,msg,from,to																										
FWB-attack	http_host,http_url,src,dst,msg,action																										
FWB-event	ui,action,msg																										
FWB-traffic	src,dst,service,http_method,msg																										
value <string>	Fields of the text search filter. Enter one or more field names separated with a comma.																										

syslog

Use this command to configure syslog servers.

Syntax

```

config system syslog
  edit <name>
    set ip <string>
    set local-cert {Fortinet_Local | Fortinet_Local2}
    set peer-cert-cn <string>
    set port <integer>
    set reliable {enable | disable}
    set secure-connection {enable | disable}
  end
end

```

Variable	Description
<name>	Syslog server name.
ip <string>	Enter the syslog server IPv4 address or hostname.
local-cert {Fortinet_Local Fortinet_Local2}	Select from the two available local certificates used for secure connection. This variable is only available when <code>secure-connection</code> is enabled.
peer-cert-cn <string>	Certificate common name of syslog server. This variable is only available when <code>secure-connection</code> is enabled. Note: Null or '-' means no certificate CN for the syslog server.
port <integer>	Enter the syslog server port (1 - 65535, default = 514).
reliable {enable disable}	Enable/disable reliable connection with syslog server (default = disable).
secure-connection {enable disable}	Enable/disable connection secured by TLS/SSL (default = disable). This variable is only available when <code>reliable</code> is enabled.

web-proxy

Use this command to configure the system web proxy.

Syntax

```
config system web-proxy
  set address <string>
  set mode {proxy | tunnel}
  set password <passwd>
  set port <integer>
  set status {enable | disable}
  set username <string>
end
```

Variable	Description
address <string>	Enter the web proxy address.
mode {proxy tunnel}	Enter the web proxy mode (default = tunnel).
password <passwd>	Enter the password for the user name used for authentication (default = *).
port <integer>	Enter the port number of the web proxy (1 - 65535, default = 1080).
status {enable disable}	Enable/disable system web proxy (default = disable).
username <string>	Enter the user name used for authentication.

fmupdate

Use `fmupdate` to configure settings related to FortiGuard service updates and the FortiAnalyzer unit's built-in FortiGuard Distribution Server (FDS).



CLI commands and variables are case sensitive.

analyzer virusreport	fds-setting	server-override-status
av-ips	fwm-setting	service
custom-url-list	multilayer	web-spam
disk-quota	publicnetwork	
fct-services	server-access-priorities	



TCP port numbers cannot be used by multiple services at the same time with the same IP address. If a port is already in use, it cannot be assigned to another service. For example, HTTPS and HTTP cannot have the same port number.

analyzer virusreport

Use this command to enable or disable notification of virus detection to Fortinet.

Syntax

```
config fmupdate analyzer virusreport
  set status {enable | disable}
end
```

Variables	Description
<code>status {enable disable}</code>	Enable/disable sending virus detection notification to FortiGuard (default = enable).

Example

This example enables virus detection notifications to Fortinet.

```
config fmupdate analyzer virusreport
  set status enable
```



```
end
```

av-ips

Use the following commands to configure antivirus settings.

av-ips advanced-log

Use this command to enable logging of FortiGuard Antivirus and IPS update packages received by the FortiAnalyzer unit's built-in FDS from the FortiGuard Distribution Network (FDN).

Syntax

```
config fmupdate av-ips advanced-log
    set log-fortigate {enable | disable}
    set log-server {enable | disable}
end
```

Variables	Description
log-fortigate {enable disable}	Enable/disable logging of FortiGuard antivirus and IPS service updates of FortiGate devices (default = disable).
log-server {enable disable}	Enable/disable logging of update packages received by the built-in FDS server (default = enable).

Example

Enable logging of FortiGuard Antivirus updates to FortiClient installations and update packages downloaded by the built-in FDS from the FDN.

```
config fmupdate av-ips advanced-log
    set log-forticlient enable
    set log-server enable
end
```

av-ips web-proxy

Use this command to configure a web proxy if FortiGuard Antivirus and IPS updates must be retrieved through a web proxy.

Syntax

```
config fmupdate av-ips web-proxy
    set address <string>
    set mode {proxy | tunnel}
    set password <password>
```

```

    set port <integer>
    set status {enable | disable}
    set username <string>
end

```

Variables	Description
address <string>	Enter the web proxy address.
mode {proxy tunnel}	Enter the web proxy mode (default = tunnel).
password <password>	If the web proxy requires authentication, enter the password for the user name (character limit = 63).
port <integer>	Enter the port number of the web proxy (1 - 65535, default = 80).
status {enable disable}	Enable/disable connections through the web proxy (default = disable).
username <string>	If the web proxy requires authentication, enter the user name (character limit = 63).

Example

You could enable a connection through a non-transparent web proxy on an alternate port.

```

config fmupdate av-ips web-proxy
    set status enable
    set mode proxy
    set address 10.10.30.1
    set port 8890
    set username avipsupdater
    set password cvhk3rf3u9jvsYU
end

```

custom-url-list

Use this command to configure the URL database for rating and filtering. You can select to use the FortiGuard URL database, a custom URL database, or both. When selecting to use a custom URL database, use the `fmupdate {ftp | scp | tftp} import` command to import the custom URL list. When FortiAnalyzer performs the URL rating, it will check the custom URL first. If a match is found, the custom rating is returned. If there is no match, then FortiAnalyzer will check the FortiGuard database.

Syntax

```

config fmupdate custom-url-list
    set db_selection {both | custom-url | fortiguard-db}
end

```

Variable	Description
db_selection {both custom-url fortiguard-db}	Manage the FortiGuard URL database: <ul style="list-style-type: none"> both: Support both custom URL database and the FortiGuard database (default) custom-url: Customer imported URL list. fortiguard-db: Fortinet's FortiGuard database

disk-quota

Use this command to configure the disk space available for use by the Upgrade Manager.

If the Upgrade Manager disk space is full or if there is insufficient space to save an update package to disk, the package will not download and an alert will be sent to notify you.

Syntax

```
config fmupdate disk-quota
    set value <size_int>
end
```

Variable	Description
value <size_int>	Configure the size of the Upgrade Manager disk quota, in megabytes (default = 51200). If you set the disk-quota smaller than the size of an update package, the update package will not download and you will get a disk full alert.

fct-services

Use this command to configure the built-in FDS to provide FortiGuard services to FortiClient installations.

Syntax

```
config fmupdate fct-services
    set status {enable | disable}
    set port <port_int>
end
```

Variables	Description
status {enable disable}	Enable/disable built-in FDS service to FortiClient installations (default = enable).
port <port_int>	Enter the port number on which the built-in FDS should provide updates to FortiClient installations (1 - 65535, default = 80).

Example

You could configure the built-in FDS to accommodate older versions of FortiClient installations by providing service on their required port.

```
config fmupdate fct-services
  set status enable
  set port 80
end
```

fds-setting

Use this command to set FDS settings.

Syntax

```
config fmupdate fds-settings
  set fds-clt-ssl-protocol {sslsv3 | tlsv1.0 | tlsv1.1 | tlsv1.2}
  set fds-ssl-protocol {sslsv3 | tlsv1.0 | tlsv1.1 | tlsv1.2}
  set fmtr-log {alert | critical | debug | disable | emergency | error | info | notice |
    warn}
  set fortiguard-anycast {enable | disable}
  set fortiguard-anycast-source {aws | fortinet}
  set linkd-log {alert | critical | debug | disable | emergency | error | info | notice |
    warn}
  set max-av-ips-version <integer>
  set max-work <integer>
  set send_report {enable | disable}
  set send_setup {enable | disable}
  set system-support-faz {6.x 7.x}
  set system-support-fct {4.x 5.0 5.2 5.4 5.6 6.0 6.2 6.4 7.0}
  set system-support-fdc {3.x 4.x}
  set system-support-fgt {5.4 5.6 6.0 6.2 6.4 7.0}
  set system-support-fml {4.x 5.x 6.0 6.2 6.4 7.0}
  set system-support-fsa {1.x 2.x 3.0 3.1 3.2 3.x 4.x}
  set system-support-fts {3.x 4.x 7.x}
  set umsvc-log {alert | critical | debug | disable | emergency | error | info | notice |
    warn}
  set unreg-dev-option {add-service | ignore | svc-only}
  set User-Agent <text>
  set wanip-query-mode {disable | ipify}
end
```

Variables	Description
<code>fds-clt-ssl-protocol {sslsv3 tlsv1.0 tlsv1.1 tlsv1.2}</code>	Set the SSL protocols version for connecting FDS server (default = tlsv1.2).
<code>fds-ssl-protocol {sslsv3 tlsv1.0 tlsv1.1 tlsv1.2}</code>	Set the SSL protocols version for FDS service (default = tlsv1.0).

Variables	Description
fmtr-log {alert critical debug disable emergency error info notice warn}	The fmtr log level. Set to <code>disable</code> to disable the log (default = info).
fortiguard-anycast {enable disable}	Enable/disable use of FortiGuard's anycast network (default = disable).
fortiguard-anycast-source {aws fortinet}	Configure which servers provide FortiGuard services in FortiGuard's anycast network (default = fortinet).
linkd-log {alert critical debug disable emergency error info notice warn}	The linkd log level (default = info).
max-av-ips-version <integer>	The maximum number of AV/IPS full version downloadable packages (default = 20).
max-work <integer>	The maximum number of worker processing downlink requests (default = 1).
send_report {enable disable}	Enable/disable sending reports to the FDS server (default = disable).
send_setup {enable disable}	Enable/disable sending setup to the FDS server (default = disable).
system-support-faz {6.x 7.x}	Set the FortiAnalyzer support version.
system-support-fct {4.x 5.0 5.2 5.4 5.6 6.0 6.2 6.4 7.0}	Set the FortiClient support version.
system-support-fdc {3.x 4.x}	Set the FortiDeceptor support version.
system-support-ftg {5.4 5.6 6.0 6.2 6.4 7.0}	Set the FortiGate support version.
system-support-fml {4.x 5.x 6.0 6.2 6.4 7.0}	Set the FortiMail support version.
system-support-fsa {1.x 2.x 3.0 3.1 3.2 3.x 4.x}	Set the FortiSandbox support version.
system-support-fts {3.x 4.x 7.x}	Set the FortiTester support version.
umsvc-log {alert critical debug disable emergency error info notice warn}	The um_service log level (default = info).
unreg-dev-option {add-service ignore svc-only}	Set the option for unregistered devices: <ul style="list-style-type: none"> <code>add-service</code>: Add unregistered devices and allow update request (default). <code>ignore</code>: Ignore all unregistered devices. <code>svc-only</code>: Allow update request without add unregistered device.
User-Agent <text>	Configure the User-Agent string.
wanip-query-mode {disable ipify}	Set the public IP query mode. <ul style="list-style-type: none"> <code>disable</code>: Do not query public IP (default) <code>ipify</code>: Get public IP through https://api.ipify.org

fds-setting push-override

Use this command to enable or disable push updates, and to override the default IP address and port to which the FDS sends FortiGuard antivirus and IPS push messages.

This is useful if push notifications must be sent to an IP address and/or port other than the FortiAnalyzer unit, such as the external or virtual IP address of a NAT device that forwards traffic to the FortiAnalyzer unit.

Syntax

```
config fmupdate fds-setting
  config push-override
    set ip <ipv_address>
    set port <integer>
    set status {enable | disable}
  end
end
```

Variable	Description
ip <ipv_address>	Enter the external or virtual IP address of the NAT device that will forward push messages to the FortiAnalyzer unit.
port <integer>	Enter the receiving port number on the NAT device (1 - 65535, default = 9443).
status {enable disable}	Enable/disable the push updates (default = disable).

Example

You could enable the FortiAnalyzer unit's built-in FDS to receive push messages.

If there is a NAT device or firewall between the FortiAnalyzer unit and the FDS, you could also notify the FDS to send push messages to the external IP address of the NAT device, instead of the FortiAnalyzer unit's private network IP address.

```
config fmupdate fds-setting
  config push-override
    set status enable
    set ip 172.16.124.135
    set port 9000
  end
end
```

You would then configure port forwarding on the NAT device, forwarding push messages received on User Datagram Protocol (UDP) port 9000 to the FortiAnalyzer unit on UDP port 9443.

fds-setting push-override-to-client

Use this command to define which FortiAnalyzer IP addresses/ports are announced to devices for which the FortiAnalyzer provides FDS services. By default, FortiAnalyzer will announce all its interfaces using the port 8890.

Syntax

```
config fmupdate fds-setting
  config push-override-to-client
    set status {enable | disable}
    config <announce-ip>
      edit <id>
        set ip <ip_address>
        set port <integer>
      end
    end
  end
```

Variable	Description
status {enable disable}	Enable/disable the push updates (default = disable).
Variables for config announce-ip subcommand:	
<id>	Edit the announce IP address ID (1 - 10).
ip <ip_address>	Enter the announce IP address.
port <integer>	Enter the announce IP port (1 - 65535, default = 8890).

fds-setting server-override

Use this command to override the default IP address and port that the built-in FDS contacts when requesting FortiGuard spam updates.

Syntax

```
config fmupdate fds-setting
  config server-override
    set status {enable | disable}
    config servlist
      edit <id>
        set ip <ipv4_address>
        set ip6 <ipv6_address>
        set port <integer>
        set server-type {fct | fds}
      end
    end
  end
```

Variable	Description
status {enable disable}	Enable/disable the override (default = disable).
Variable for config servlist subcommand:	
<id>	Enter the override server ID (1 - 10).
ip <ipv4_address>	Enter the IPv4 address of the override server address.

Variable	Description
ip6 <ipv6_address>	Enter the IPv6 address of the override server address.
port <integer>	Enter the port number to use when contacting the FDS (1 - 65535, default = 443).
server-type {fct fds}	Set the override server type (default = fds).

fds-setting update-schedule

Use this command to schedule when the built-in FortiGuard retrieves antivirus and IPS updates.

Syntax

```
config fmupdate fds-setting
  config update-schedule
    set day {Sunday | Monday | Tuesday | Wednesday | Thursday | Friday | Saturday}
    set frequency {every | daily | weekly}
    set status {enable | disable}
    set time <hh:mm>
  end
end
```

Variable	Description
day {Sunday Monday Tuesday Wednesday Thursday Friday Saturday}	The day that the update will occur (Sunday - Saturday, default = Monday). This option is only available if the update frequency is <code>weekly</code> .
frequency {every daily weekly}	The update frequency: every given time interval, once a day, or once a week (default = <code>every</code>).
status {enable disable}	Enable/disable scheduled updates (default = <code>enable</code>).
time <hh:mm>	The time interval between updates, or the hour and minute when the update occurs (hh: 0 - 23, mm: 0 - 59 or 60 = random, default = 00:10).

fwm-setting

Use this command to configure firmware management settings.

Syntax

```
config fmupdate fwm-setting
  set auto-scan-fgt-disk {enable | disable}
  set check-fgt-disk {enable | disable}
  set fds-failover-fmg {enable | disable}
  set fds-image-timeout <integer>
  set immx-source {cloud | fgt | fmg}
  set log {fwm | fwm_dm | fwm_dm_json}
```



```

set multiple-steps-interval <integer>
set retry-interval <integer>
set retry-max <integer>
config upgrade-timeout
    set check-status-timeout <integer>
    set ctrl-check-status-timeout <integer>
    set ctrl-put-image-by-fds-timeout <integer>
    set ha-sync-timeout <integer>
    set license-check-timeout <integer>
    set prepare-image-timeout <integer>
    set put-image-by-fds-timeout <integer>
    set put-image-timeout <integer>
    set reboot-of-fsck-timeout <integer>
    set reboot-of-upgrade-timeout <integer>
    set retrieve-timeout <integer>
    set rpc-timeout <integer>
    set total-timeout <integer>
end
end

```

Variable	Description
auto-scan-fgt-disk {enable disable}	Enable/disable automatic scanning of a FortiGate disk when required (default = enable).
check-fgt-disk {enable disable}	Enable/disable checking a FortiGate disk prior to upgrading the image (default = enable).
fds-failover-fmg {enable disable}	Enable/disable using the a local image file on the FortiManager when the FDS download fails (default = enable).
fds-image-timeout <integer>	Set the timer for FortiGate image downloads from FortiGuard, in seconds (300 - 3600, default = 1800).
immx-source {cloud fgt fmg}	Configure which of the IMMX file to be used for choosing the upgrade patch: <ul style="list-style-type: none"> cloud: Use the IMMX file for FortiCloud. fgt: Use the IMMX file for FortiGate. fmg: Use the IMMX file for FortiManager. The default file is the one for FortiManager (default = fmg).
log {fwm fwm_dm fwm_dm_json}	Configure log setting for the firmware manager daemon (default = fwm_dm): <p>fwm: Firmware Manager daemon log.</p> <p>fwm_dm: Firmware Manager and deployment service log.</p> <p>fwm_dm_json: Firmware Manager and Deployment service log with JSON data between FortiManager-FortiGate.</p>
multiple-steps-interval <integer>	Set the waiting time between multiple step upgrades, in seconds (30 - 180, default = 60).
retry-interval <integer>	Waiting time for resending request to device (1 - 360, default = 60).
retry-max <integer>	Maximum number of retries for sending request to device (0 - 100, default = 10).
Variables for config upgrade-timeout subcommand:	

Variable	Description
check-status-timeout <integer>	Set the timeout for checking status after tunnel is up, in seconds. (1 - 6000, default = 600)
ctrl-check-status-timeout <integer>	Set the timeout for checking FortiAP/FortiSwitch/FortiExtender status after request upgrade, in seconds. (1 - 12000, default = 1200)
ctrl-put-image-by-fds-timeout <integer>	Set the timeout for waiting device get FortiAP/FortiSwitch/FortiExtender image from FortiGuard, in seconds. (1 - 9000, default = 900)
ha-sync-timeout <integer>	Set the timeout for waiting HA sync, in seconds. (1 - 18000, default = 1800)
license-check-timeout <integer>	Set the timeout for waiting FortiGate check license, in seconds. (1 - 6000, default = 600)
prepare-image-timeout <integer>	Set the timeout for preparing image, in seconds. (1 - 6000, default = 600)
put-image-by-fds-timeout <integer>	Set the timeout for waiting device get image from FortiGuard, in seconds. (1 - 18000, default = 1800)
put-image-timeout <integer>	Set the timeout for waiting send image over tunnel, in seconds. (1 - 18000, default = 1800)
reboot-of-fsck-timeout <integer>	Set the timeout for waiting FortiGate reboot, in seconds. (1 - 18000, default = 1800)
reboot-of-upgrade-timeout <integer>	Set the timeout for waiting FortiGate reboot after image upgrade, in seconds. (1 - 12000, default = 1200)
retrieve-timeout <integer>	Set the timeout for waiting retrieve, in seconds. (1 - 18000, default = 1800)
rpc-timeout <integer>	Set the timeout for waiting FortiGate rpc response, in seconds. (1 - 1800, default = 180)
total-timeout <integer>	Set the timeout for the whole FortiGate upgrade, in seconds. (1 - 86400, default = 3600)

multilayer

Use this command to set multilayer mode configuration.

Syntax

```
config fmupdate multilayer
    set webspam-rating {enable | disable}
end
```

Variables	Description
webspam-rating {enable disable}	Enable/disable URL/antispam rating service (default = enable).

publicnetwork

Use this command to enable access to the public FDS. If this function is disabled, the service packages, updates, and license upgrades must be imported manually.

Syntax

```
config fmupdate publicnetwork
    set status {enable | disable}
end
```

Variables	Description
status {enable disable}	Enable/disable the public network (default = enable).

server-access-priorities

Use this command to configure how a FortiGate unit may download antivirus updates and request web filtering services from multiple FortiAnalyzer units and private FDS servers.

Use the `private-server` subcommand to configure multiple FortiAnalyzer units and private servers.



By default, the FortiGate unit receives updates from the FortiAnalyzer unit if the FortiGate unit is managed by the FortiAnalyzer unit and the FortiGate unit was configured to receive updates from the FortiAnalyzer unit.

Syntax

```
config fmupdate server-access-priorities
    set access-public {enable | disable}
    set av-ips {enable | disable}
    set web-spam {enable | disable}
    config private-server
        edit <id>
            set ip <ipv4_address>
            set ip6 <ipv6_address>
            set time_zone <integer>
        end
    end
end
```

Variables	Description
access-public {enable disable}	Enable/disable allowing FortiGates to access public FortiGuard servers when private servers are unavailable (default = disable).
av-ips {enable disable}	Enable/disable receiving antivirus and IPS update service for private servers (default = disable).

Variables	Description
web-spam {enable disable}	Enable/disable Web Filter and Email Filter update service for private servers (default = enable).
Variables for <code>config private-server</code> subcommand:	
<id>	Enter a number to identify the FortiManager unit or private server (1 - 10).
ip <ipv4_address>	Enter the IPv4 address of the FortiManager unit or private server.
ip6 <ipv6_address>	Enter the IPv6 address of the FortiManager unit or private server.
time_zone <integer>	Enter the correct time zone of the private server (-24 = local time zone, default = -24).

Example

The following example configures access to public FDS servers and allows FortiGate units to receive antivirus updates from other FortiAnalyzer units and private FDS servers. This example also configures two private servers.

```
config fmupdate server-access-priorities
  set access-public enable
  set av-ips enable
  config private-server
    edit 1
      set ip 172.16.130.252
    next
    edit 2
      set ip 172.31.145.201
    end
  end
end
```

server-override-status

Configure strict or loose server override.

Syntax

```
config fmupdate server-override-status
  set mode {loose | strict}
end
```

Variables	Description
mode {loose strict}	Set the server override mode: <ul style="list-style-type: none"> loose: Allow access other servers (default). strict: Access override server only.

service

Use this command to enable or disable the services provided by the built-in FDS.

Syntax

```
config fmupdate service
  set avips {enable | disable}
end
```

Variables	Description
avips {enable disable}	Enable/disable the built-in FortiGuard to provide FortiGuard antivirus and IPS updates (default = enable).

Example

```
config fmupdate service
  set avips enable
end
```

web-spam

Use the following commands to configure FortiGuard antispam related settings.

web-spam fgd-setting

Use this command to configure FortiGuard run parameters.

Syntax

```
config fmupdate web-spam fgd-setting
  set as-cache <integer>
  set as-log {all | disable | nospam}
  set as-preload {enable | disable}
  set av-cache <integer>
  set av-log {all | disable | novirus}
  set av-preload {enable | disable}
  set av2-cache <integer>
  set av2-log {all | disable | noav2}
  set av2-preload {enable | disable}
  set eventlog-query {enable | disable}
  set fgd-pull-interval <integer>
  set fq-cache <integer>
  set fq-log {all | disable | nofilequery}
  set fq-preload {enable | disable}
```

```

set iot-cache <integer>
set iot-log {all | disable | nofilequery}
set iot-preload {enable | disable}
set linkd-log {enable | disable}
set max-client-worker <integer>
set max-log-quota <integer>
set max-unrated-size <integer>
set restrict-as1-dbver <string>
set restrict-as2-dbver <string>
set restrict-as4-dbver <string>
set restrict-av-dbver <string>
set restrict-av2-dbver <string>
set restrict-fq-dbver <string>
set restrict-iots-dbver <string>
set restrict-wf-dbver <string>
set stat-log {alert | critical | debug | disable | emergency | error | info | notice |
    warn}
set stat-log-interval <integer>
set stat-sync-interval <integer>
set update-interval <integer>
set update-log {enable | disable}
set wf-cache <integer>
set wf-dn-cache-expire-time <integer>
set wf-dn-cache-max-number <integer>
set wf-log {all | disable | nouri}
set wf-preload {enable | disable}
config server-override
    set status {enable | disable}
    config servlist
        edit <id>
            set ip <ipv4_address>
            set ip6 <ipv6_address>
            set port <integer>
            set service-type {fgc | fgd | fsa}
        end
    end
end

```

Variable	Description
as-cache <integer>	Antispam service maximum memory usage in megabytes (Maximum = Physical memory-1024, 0 = no limit, default = 300).
as-log {all disable nospam}	Antispam log setting: <ul style="list-style-type: none"> all: Log all spam lookups. disable: Disable spam log. nospam: Log non-spam events (default)
as-preload {enable disable}	Enable/disable preloading the antispam database into memory (default = disable).
av-cache <integer>	Antivirus service maximum memory usage, in megabytes (100 - 500, default = 300).
av-log {all disable novirus}	Antivirus log setting: <ul style="list-style-type: none"> all: Log all virus lookups.

Variable	Description
	<ul style="list-style-type: none"> <code>disable</code>: Disable virus log. <code>novirus</code>: Log non-virus events (default).
<code>av-preload {enable disable}</code>	Enable/disable preloading antivirus database to memory (default = disable).
<code>av2-cache <integer></code>	Antispam service maximum memory usage, in megabytes (physical memory to 1024, 0 = no limit, default = 800).
<code>av2-log {all disable novirus}</code>	Outbreak prevention log setting: <ul style="list-style-type: none"> <code>all</code>: Log all av2 lookups. <code>disable</code>: Disable av2 logs. <code>noav2</code>: Log non-av2 events (default).
<code>av2-preload {enable disable}</code>	Enable/disable preloading outbreak prevention database to memory (default = disable).
<code>eventlog-query {enable disable}</code>	Enable/disable record query to event-log besides fgd-log (default = disable).
<code>fgd-pull-interval <integer></code>	FortiGuard pull interval setting, in minutes (1 - 1440, default = 10).
<code>fq-cache <integer></code>	File query service maximum memory usage, in megabytes (100 - 500, default = 300).
<code>fq-log {all disable nofilequery}</code>	Filequery log setting: <ul style="list-style-type: none"> <code>all</code>: Log all file query. <code>disable</code>: Disable file query log. <code>nofilequery</code>: Log non-file query events (default).
<code>fq-preload {enable disable}</code>	Enable/disable preloading the filequery database to memory (default = disable).
<code>iot-cache <integer></code>	IoT service maximum memory usage, in megabytes (100 - 500, default = 300).
<code>iot-log {all disable nofilequery}</code>	IoT log setting (default = nofilequery).
<code>iot-preload {enable disable}</code>	Enable/disable preloading IoT database to memory (default = disable).
<code>linkd-log {enable disable}</code>	Linkd log setting: <ul style="list-style-type: none"> <code>alert</code>: Immediate action is required. <code>critical</code>: Functionality is affected. <code>debug</code>: Debug information (default). <code>disable</code>: Linkd logging is disabled. <code>emergency</code>: The unit is unusable. <code>error</code>: Functionality is probably affected. <code>info</code>: General information. <code>notice</code>: Information about normal events. <code>warn</code>: Functionality might be affected.
<code>max-client-worker <integer></code>	Maximum workers to use for TCP client connections (0 - 16, 0 = use CPU count, default = 0).
<code>max-log-quota <integer></code>	Maximum log quota setting, in megabytes (100 - 20480, default = 6144).

Variable	Description
max-unrated-size <integer>	Maximum number of unrated site in memory, in kilobytes(10 - 5120, default = 500).
restrict-as1-dbver <string>	Restrict system update to indicated antispam(1) database version (character limit = 127).
restrict-as2-dbver <string>	Restrict system update to indicated antispam(2) database version (character limit = 127).
restrict-as4-dbver <string>	Restrict system update to indicated antispam(4) database version (character limit = 127).
restrict-av-dbver <string>	Restrict system update to indicated antivirus database version (character limit = 127).
restrict-av2-dbver <string>	Restrict system update to indicated outbreak prevention database version (character limit = 127).
restrict-fq-dbver <string>	Restrict system update to indicated file query database version (character limit = 127).
restrict-iots-dbver <string>	Restrict system update to indicated file query database version (character limit = 127).
restrict-wf-dbver <string>	Restrict system update to indicated web filter database version (character limit = 127).
stat-log {alert critical debug disable emergency error info notice warn}	Statistic log setting (default = disable). <ul style="list-style-type: none"> • alert: Immediate action is required (1). • critical: Functionality is affected (2). • debug: Debug information (7). • disable: Linkd logging is disabled. • emergency: The unit is unusable (0). • error: Functionality is probably affected (3). • info: General information (6). • notice: Information about normal events (5). • warn: Functionality might be affected (4).
stat-log-interval <integer>	Statistic log interval setting, in minutes (1 - 1440, default = 60).
stat-sync-interval <integer>	Synchronization interval for statistic of unrated site in minutes (1 - 60, default = 60).
update-interval <integer>	FortiGuard database update wait time if not enough delta files, in hours (2 - 24, default = 6).
update-log {enable disable}	Enable/disable update log setting (default = enable).
wf-cache <integer>	Web filter service maximum memory usage, in megabytes (maximum = Physical memory-1024, 0 = no limit, default = 600).
wf-dn-cache-expire-time	Web filter DN cache expire time, in minutes (1 - 1440, 0 = never, default = 30).

Variable	Description
wf-dn-cache-max-number	Maximum number of Web filter DN cache (0 = disable, default = 10000).
wf-log {all disable nouri}	Web filter log setting: <ul style="list-style-type: none"> all: Log all URL lookups. disable: Disable URL log. nouri: Log non-URL events (default).
wf-preload {enable disable}	Enable/disable preloading the web filter database into memory (default = disable).
Variables for <code>config server-override</code> subcommand:	
status {enable disable}	Enable/disable the override (default = disable).
<id>	Override server ID (1 - 10).
ip <ipv4_address>	IPv4 address of the override server.
ip6 <ipv6_address>	IPv6 address of the override server.
port <integer>	Port number to use when contacting FortiGuard (1 - 65535, default = 443).
service-type {fgc fgd fsa}	Override service type.

web-spam web-proxy

Use this command to configure the web-spam web-proxy.

Syntax

```
config fmupdate web-spam web-proxy
  set address <string>
  set mode {proxy | tunnel}
  set password <passwd>
  set port <integer>
  set status {enable | disable}
end
```

Variable	Description
address <string>	Enter the web proxy address.
mode {proxy tunnel}	Enter the web proxy mode (default = tunnel).
password <passwd>	If the web proxy requires authentication, type the password for the user name.
port <integer>	Enter the port number of the web proxy (1- 65535, default = 80).
status {enable disable}	Enable/disable connections through the web proxy (default = disable).
username <string>	If the web proxy requires authentication, enter the user name.

fortirecorder

Use `fortirecorder` to configure settings related to FortiRecorder.



These commands are only available on hardware-based FortiAnalyzer models.



CLI commands and variables are case sensitive.

camera

global

schedule

camera

Use this command to configure FortiRecorder camera settings.



This command is only available on hardware-based FortiAnalyzer models.

camera devices

Configure camera information. The available options will vary depending on the camera model selected.

Syntax

```
config fortirecorder camera devices
edit <device>
    set addr <string>
    set address-mode wired
    set alarm-post <integer>
    set alarm-pre <integer>
    set audio-bitrate <integer>
    set audio-codec <string>
    set audio-detect-sensitivity
    set audio-input {default | line | mic}
```

```
set audio-input-level <integer>
set audio-output
set audio-output-echo-cancel
set audio-output-level <integer>
set audio-output-mute
set audio-samplerate <integer>
set camera-type managed
set comm-http-port <integer>
set comm-https-port <integer>
set comm-type {http | https}
set digital-input
set digital-output
set exposure-environment {indoor | outdoor}
set exposure-gain-max
set exposure-shutter-min {2 | 4 | 8 | 15 | 30}
set exposure-wdr-digital {on | off | 1 | 2 | 3}
set exposure-wdr-shutter {off | 1 | 2}
set face-recognition {enable | disable}
set fw-version
set image-digital-zoom
set image-dis
set image-dnr {auto | manual | off}
set image-dnr-level <integer>
set index
set infrared-disable-threshold <integer>
set infrared-dwell-time
set infrared-enable-threshold <integer>
set infrared-led {auto | off}
set infrared-led-intensity {auto | fixed}
set infrared-led-level
set infrared-mode {auto | off}
set light-detection pir
set light-disable-threshold
set light-dwell-time
set light-enable-threshold
set light-mode
set location <string>
set login-password
set mac
set model-name <model>
set move-home
set move-home-delay <integer>
set move-home-pan <integer>
set move-home-tilt <integer>
set move-home-zoom <integer>
set operator-password
set overlay-mode {off | name time-date gmt}
set pir-sensitivity
set port <integer>
set privacy-button {enable | disable}
set profile <string>
set push-config {enable | disable}
set ready {enable | disable}
set status {enable | disable}
set status-led {enable | disable}
set tamper-detect-sensitivity
set transport-http-port <integer>
```

```

set transport-https-port <integer>
set transport-tcp-port <integer>
set transport-type {http | tcp | udp}
set transport-udp-port <integer>
set unready-state
set unready-state-detail
set vendor-name
set video-aspect {sd | hd}
set video-brightness <integer>
set video-contrast <integer>
set video-orientation {normal | vertical | horizontal | rotate-90 | rotate-180 |
    rotate-270}
set video-saturation <integer>
set video-sharpness <integer>
set view-angle
set wired-addr <ip4|ip6>
set wired-gateway <ip4|ip6>
set wired-mode {dhcp | static}
set wired-netmask <ip4|ip6>
set wired-primary-dns <ip4|ip6>
set wired-secondary-dns <ip4|ip6>
set zoom <integer>
config motion
    edit <motion>
        set motion-pixel <integer>
        set motion-sensitivity <integer>
        set motion-top <integer>
        set motion-left <integer>
        set motion-bottom <integer>
        set motion-right <integer>
    next
end
config mask
    edit <mask>
        set mask-top <integer>
        set mask-left <integer>
        set mask-bottom <integer>
        set mask-right <integer>
    next
end
config ptz-presets
    edit <preset>
        set pan <integer>
        set tilt <integer>
        set zoom <integer>
    next
end
next
end

```

Variable	Description
<device>	Enter the name of the device you need to edit.
addr <string>	The camera address as configured on the camera.

Variable	Description
address-mode wired	How that camera is reached.
alarm-post <integer>	Set the capture time after an alarm, in seconds (0 - 300, default = 30).
alarm-pre <integer>	Set the capture time before an alarm, in seconds (0 - 10, default = 10).
audio-bitrate <integer>	Set the audio bitrate (default = 64000). This option is only available for camera models that have audio capabilities.
audio-codec <string>	Set the audio codec. This option is only available for camera models that have audio capabilities.
audio-detect-sensitivity	
audio-input {default line mic}	Set the audio input source. This option is only available for camera models that have audio input capabilities.
audio-input-level <integer>	Set the audio input level (1 - 100, default = 60). This option is only available for camera models that have audio input capabilities.
audio-output	
audio-output-echo-cancel	
audio-output-level <integer>	Set the audio output level (1 - 100, default = 60). This option is only available for camera models that have audio output capabilities.
audio-output-mute	
audio-samplerate <integer>	Set the audio sample rate. This option is only available for camera models that have audio capabilities.
camera-type managed	The camera type.
comm-http-port <integer>	Set the command HTTP port (0 - 65535, default = 0).
comm-https-port <integer>	Set the command HTTPS port (0 - 65535, default = 0).
comm-type {http https}	Set the command protocol (default = http).
digital-input	
digital-output	
exposure-environment {indoor outdoor}	Set the exposure environment (default = indoor).
exposure-gain-max	
exposure-shutter-min {2 4 8 15 30}	Set the minimum shutter speed. <ul style="list-style-type: none"> 2: 1/2 seconds (default) 4: 1/4 seconds 8: 1/8 seconds 15: 1/15 seconds 30: 1/30 seconds

Variable	Description
exposure-wdr-digital {on off 1 2 3}	Turn on/off exposure digital wide dynamic, or set its value (default = off). The available options depend on the camera model.
exposure-wdr-shutter {off 1 2}	Set the exposure digital wide dynamic shutter speed (default = off).
face-recognition {enable disable}	Enable\disable facial recognition (default = disable).
fw-version	
image-digital-zoom	
image-dis	
image-dnr {auto manual off}	Turn on/off image digital noise reduction (default = off).
image-dnr-level <integer>	Image Digital Noise Reduction (DNR) manual level (1 - 10, default = 1). This option is only available when <code>image-dnr</code> is <code>manual</code> .
index	
infrared-disable-threshold <integer>	Set the infrared disable threshold (0 - 100, default = 15)
infrared-dwell-time	Set the infrared dwell time, in seconds (0 - 300, default = 5).
infrared-enable-threshold <integer>	Set the infrared enable threshold (0 - 100, default = 5)
infrared-led {auto off}	Set the infrared LED status (default = auto).
infrared-led-intensity {auto fixed}	Set the infrared LED intensity (default = auto).
infrared-led-level	
infrared-mode {auto off}	Configure infrared mode (default = auto). The available options depend on the camera model.
light-detection pir	Set light detection to Passive Infrared (PIR) sensor.
light-disable-threshold	
light-dwell-time	
light-enable-threshold	
light-mode	
location <string>	Set the camera location.
login-password	
mac	
model-name <model>	Set the camera model name.
move-home	

Variable	Description
move-home-delay <integer>	Set the amount of time of inactivity before the camera moves to its home position, in minutes (1 - 60, default = 5).
move-home-pan <integer>	
move-home-tilt <integer>	
move-home-zoom <integer>	
operator-password	
overlay-mode {off name time-date gmt}	Set the text overlay mode (default = name time-date gmt).
pir-sensitivity	
port <integer>	Set the camera command port (0 - 65535, default = 0).
privacy-button {enable disable}	Enable/disable the privacy button (default = disable).
profile <string>	Set the camera profile.
push-config {enable disable}	Enable/disable pushing the configuration.
ready {enable disable}	
status {enable disable}	Enable/disable the camera (default = enable).
status-led {enable disable}	Enable/disable the LED on the camera (default = disable).
tamper-detect-sensitivity	
transport-http-port <integer>	Set the HTTP transport port (0 - 65535, default = 0).
transport-https-port <integer>	Set the HTTPS transport port (0 - 65535, default = 0).
transport-tcp-port <integer>	Set the TCP transport port (0 - 65535, default = 0).
transport-type {http https tcp udp}	Set the transport type to get media from the camera. The available options will vary depending on the camera model.
transport-udp-port <integer>	Set the UDP transport port (0 - 65535, default = 0).
unready-state	
unready-state-detail	
vendor-name	
video-aspect {sd hd}	Set the video aspect ration. The available options will vary depending on the camera model.
video-brightness <integer>	Set the video brightness (0 - 100, default = 50).
video-contrast <integer>	Set the video contrast (0 - 100, default = 50).

Variable	Description
video-orientation {normal vertical horizontal rotate-90 rotate-180 rotate-270}	Set the video orientation (default = normal).
video-saturation <integer>	Set the video saturation (0 - 100, default = 50).
video-sharpness <integer>	Set the video sharpness (0 - 100, default = 50).
view-angle	
wired-addr <ip4 ip6>	Set the camera IP address. This option is only available when address-mode is wired and wired-mode is static.
wired-gateway <ip4 ip6>	Set the camera gateway. This option is only available when address-mode is wired and wired-mode is static.
wired-mode {dhcp static}	Set the IP address assignment mode (default = dhcp).
wired-netmask <ip4 ip6>	Set the camera netmask. This option is only available when address-mode is wired and wired-mode is static.
wired-primary-dns <ip4 ip6>	Set the primary DNS. This option is only available when address-mode is wired and wired-mode is static.
wired-secondary-dns <ip4 ip6>	Set the secondary DNS. This option is only available when address-mode is wired and wired-mode is static.
zoom <integer>	Set the zoom level (0 - 100, default = 0)
Variables for config motion subcommand:	
<motion>	Enter the motion number (0 - 100).
motion-pixel <integer>	Set the pixel percentage change for motion detection (0 - 100, default = 10).
motion-sensitivity <integer>	Set the sensitivity for motion detection (0 - 100, default = 80).
motion-top <integer>	Set the top percentage of the motion detection window (0 - 100, default = 0).
motion-left <integer>	Set the left percentage of the motion detection window (0 - 100, default = 0).
motion-bottom <integer>	Set the bottom percentage of the motion detection window (0 - 100, default = 100).
motion-right <integer>	Set the right percentage of the motion detection window (0 - 100, default = 100).
Variables for config mask subcommand:	
<mask>	Enter the mask number (0 - 100).
mask-top <integer>	Set the top percentage of privacy mask (0 - 100, default = 0).
mask-left <integer>	Set the left percentage of privacy mask (0 - 100, default = 0).
mask-bottom <integer>	Set the bottom percentage of privacy mask (0 - 100, default = 100).
mask-right <integer>	Set the right percentage of privacy mask (0 - 100, default = 100).
Variables for config ptz-presets subcommand:	

Variable	Description
<preset>	Enter the preset name.
pan <integer>	Set the pan value (default = 0).
tilt <integer>	Set the pan value (default = 0).
zoom <integer>	Set the pan value (default = 0).

camera profile

Configure camera profiles.

Syntax

```

config fortirecorder camera profile
  edit <profile>
    set continuous-retention-disposition {delete | keep}
    set continuous-retention-period <integer>
    set continuous-retention-period-units {days | hours | weeks | months | years}
    set detection-retention-disposition {delete | keep | virtual}
    set detection-retention-period <integer>
    set detection-retention-period-units {days | hours | weeks | months | years}
    config recording-schedule
      edit <schedule>
        set record-type {continuous motion-detect | none}
        set store-on
        set temporary-stream-for-video-clips {if-needed | no | yes}
      next
    end
  config video-schedule
    edit <schedule>
      set recording-stream <string>
      set viewing-stream <string>
    next
  end
next
end

```

Variable	Description
<profile>	Enter the profile name of the entry you need to edit or type a new name to create a new profile (character limit = 127).
continuous-retention-disposition {delete keep}	Keep or delete continuous recordings (default = keep).
continuous-retention-period <integer>	The period to keep continuous recordings (0 = forever, default = 1). This option is only available when continuous-retention-disposition is delete.

Variable	Description
continuous-retention-period-units {days hours weeks months years}	The period unit for continuous recording retention (default = months). This option is only available when continuous-retention-disposition is delete.
detection-retention-disposition {delete keep virtual}	Keep or delete detection recordings (default = keep).
detection-retention-period <integer>	The period to keep detection recordings (0 = forever, default = 1). This option is only available when detection-retention-disposition is delete.
detection-retention-period-units {days hours weeks months years}	The period unit for detection recording retention (default = months). This option is only available when detection-retention-disposition is delete.
Variables for config recording-schedule subcommand:	
<schedule>	Select a schedule. To create a schedule use the config fortirecorder schedule command.
record-type {continuous motion-detect none}	Set the recording type (default = continuous).
store-on	
temporary-stream-for-video-clips {if-needed no yes}	Use a temporary stream for video clip creation (default = if-needed).
Variables for config video-schedule subcommand:	
<schedule>	Select a schedule. To create a schedule use the config fortirecorder schedule command.
recording-stream <string>	Select the video profile for the recording stream.
viewing-stream <string>	Select the video profile for the viewing stream.

camera video

Configure camera video profiles.

Syntax

```
config fortirecorder camera video profile
edit <profile>
    set audio {enable | disable}
    set video-bitrate {fixed | variable}
    set video-bitrate-mode {fixed | variable}
    set video-codec {default | h264 | h265}
    set video-fps <integer>
    set video-quality {extra-high | high | normal | low | extra-low}
    set video-resolution {1mp | 2mp | 3mp | 4mp | 5mp | 6mp | extra-high | half_mp |
        high | low | medium}
next
end
```

Variable	Description
audio {enable disable}	Enable/disable audio (default = disable).
video-bitrate {fixed variable}	Set the bitrate (default = variable).
video-bitrate-mode {fixed variable}	Set the bitrate mode (default = variable).
video-codec {default h264 h265}	Set the video codec (default = default).
video-fps <integer>	Set the frames per second (FPS) of the video (1 - 60, default = 30).
video-quality {extra-high high normal low extra-low}	Set the video quality (default = extra-high).
video-resolution {1mp 2mp 3mp 4mp 5mp 6mp extra-high half_mp high low medium}	Set the video resolution (default = medium).

global

Use this command to configure global FortiRecorder settings.



This command is only available on hardware-based FortiAnalyzer models.

Syntax

```
config fortirecorder global
  set camera-key <string>
  set ftp-password <string>
  set public-address <string>
  set public-ftp-port <integer>
  set public-http-port <integer>
  set public-https-port <integer>
  set public-notify-http-port <integer>
  set public-notify-tcp-port <integer>
  set public-rtsp-port <integer>
end
```

Variable	Description
camera-key <string>	Key for generating camera admin and operator passwords.
ftp-password <string>	Set the FTP password.

Variable	Description
public-address <string>	Set the public address of the FortiRecorder.
public-ftp-port <integer>	Set the public FTP port of the FortiRecorder (default = 21).
public-http-port <integer>	Set the public HTTP port of the FortiRecorder (default = 80).
public-https-port <integer>	Set the public HTTPS port of the FortiRecorder (default = 443).
public-notify-http-port <integer>	Set the public notify HTTP port of the FortiRecorder (default = 3011).
public-notify-tcp-port <integer>	Set the public notify TCP port of the FortiRecorder (default = 3010).
public-rtsp-port <integer>	Set the public RTSP port of the FortiRecorder (default = 554).

schedule

Use this command to configure the FortiRecorder schedule object settings.



This command is only available on hardware-based FortiAnalyzer models.

Syntax

```
config fortirecorder schedule object
edit <schedule>
    set all-day {enable | disable}
    set date-end <string>
    set date-start <string>
    set days {su mo tu we th fr sa}
    set description <string>
    set end-time-type time
    set start-time-type time
    set time-end <string>
    set time-start <string>
    set type {one-time | recurring}
next
end
```

Variable	Description
<schedule>	Enter the schedule name of the entry you need to edit or type a new name to create a new schedule (character limit = 127).
all-day	Enable/disable all day event (default = enable).
date-end <string>	Set the schedule end date (YYYY-MM-DD). This option is only available when the schedule type is <code>one-time</code> .

Variable	Description
date-start <string>	Set the schedule start date (YYYY-MM-DD). This option is only available when the schedule type is <code>one-time</code> .
days {su mo tu we th fr sa}	Set the days that the schedule occurs on (default = su mo tu we th fr sa). This option is only available when the schedule type is <code>recurring</code> .
description <string>	A description of the schedule.
end-time-type time	The end time type (default - time). This option is only available when <code>all-day</code> is disabled.
start-time-type time	The start time type (default - time). This option is only available when <code>all-day</code> is disabled.
time-end <string>	The schedule end time (HH-MM). This option is only available when <code>all-day</code> is disabled.
time-start <string>	The schedule start time (HH-MM). This option is only available when <code>all-day</code> is disabled.
type {one-time recurring}	The schedule type (default = recurring).

execute

The `execute` commands perform immediate operations on the FortiAnalyzer unit. You can:

- Back up and restore the system settings, or reset the unit to factory settings.
- Set the unit date and time.
- Use ping to diagnose network problems.
- View the processes running on the FortiAnalyzer unit.
- Start and stop the FortiAnalyzer unit.
- Reset or shut down the FortiAnalyzer unit.



FortiAnalyzer CLI commands and variables are case sensitive.

add-mgmt-license	fmupdate	ping	sql-query-generic
add-on-license	format	ping6	sql-report
add-vm-license	fortirecorder	raid	ssh
backup	iotop	reboot	ssh-known-hosts
bootimage	iotps	remove	tac
certificate	log	reset	time
console	log-aggregation	restore	top
date	log-fetch	sensor	traceroute
device	log-integrity	shutdown	traceroute6
erase-disk	lvm	sql-local	
factory-license	migrate	sql-query-dataset	

add-mgmt-license

Use this command to load management licenses to the FortiAnalyzer.



This command is only available on hardware-based FortiAnalyzer models.

Syntax

```
execute add-mgmt-license <mgmt license string>
```

Variable	Description
<mgmt license string>	The license string. Copy and paste the string from the license file. The license string must be enclosed with double quotes. Do not removed line breaks from the string.

Example

The contents of the license file needs to be in quotes in order for it to work.

```
execute add-mgmt-license "-----BEGIN FAZ MGMT LICENSE-----  
QAAAAJ09s+LTe...ISJTTYpCKoDmMa6  
-----END FAZ MGMT LICENSE-----"
```

add-on-license

Use this command to load add-on licenses to support more devices or ADOMs with a license key.

Syntax

```
execute add-on-license <license>
```

Variable	Description
<license>	The add-on license string. Copy and paste the string from the license file. The license string must be enclosed with double quotes. Do not removed line breaks from the string.

add-vm-license

Add a VM license to the FortiAnalyzer.

Syntax

```
execute add-vm-license <vm license string>
```

Variable	Description
<vm license string>	The VM license string. Copy and paste the string from the license file. The license string must be enclosed with double quotes. Do not removed line breaks from the string.

Example

The contents of the license file needs to be in quotes in order for it to work.

```
execute add-vm-license "-----BEGIN FAZ VM LICENSE-----
QAAAAJ09s+LTe...ISJTTYpCKoDmMa6
-----END FAZ VM LICENSE-----"
```



This command is only available on FortiAnalyzer VM models.

backup

Use the following commands to backup all settings or logs on your FortiAnalyzer.

When you back up the unit settings from the vdom_admin account, the backup file contains global settings and the settings for each VDOM. When you back up the unit settings from a regular administrator account, the backup file contains the global settings and only the settings for the VDOM to which the administrator belongs.

An MD5 checksum is automatically generated in the event log when backing up the configuration. You can verify a backup by comparing the checksum in the log entry with that of the backup file.

Syntax

```
execute backup all-settings {ftp | scp | sftp} <ip:port> <string> <username> <passwd>
<ssh-cert> [crptpasswd] [force-docker]
execute backup logs <device name(s)> {ftp | scp | sftp} <ip> <username> <passwd>
<directory> [vdlist]
execute backup logs-only <device name(s)> {ftp | scp | sftp} <ip> <username> <passwd>
<directory> [vdlist]
execute backup logs-rescue <device serial number(s)> {ftp | scp | sftp} <ip> <username>
<passwd> <directory> [vdlist]
execute backup reports <report schedule name(s)> {ftp | scp | sftp} <ip> <username>
<passwd> <directory> [vdlist]
execute backup reports-config <adom name(s)> {ftp | scp | sftp} <ip> <username> <passwd>
<directory> [vdlist]
```

Variable	Description
all-settings	Backup all FortiAnalyzer settings to a file on a server.

Variable	Description
logs	Backup the device logs and the content archives to a specified server.
logs-only	Backup device logs excluding content archives to a specified server.
logs-rescue	Use this hidden command to backup logs regardless of DVM database for emergency reasons. This command will scan folders under /Storage/Logs/ for possible device logs to backup.
reports	Backup the reports to a specified server.
reports-config	Backup reports configuration to a specified server.
<device name(s)>	Enter the device name(s) separated by a comma, or enter <code>all</code> for all devices.
<device serial number(s)>	Enter the device serial number(s) separated by a comma, or enter <code>all</code> for all devices.
<report schedule name(s)>	Enter the report schedule name(s) separated by a comma, or enter <code>all</code> for all reports schedules.
<adom name(s)>	Enter the ADOM name(s) separated by a comma, or enter <code>all</code> for all ADOMs.
{ftp scp sftp}	Enter the server type: <code>ftp</code> , <code>scp</code> , or <code>sftp</code> .
<ip:port>	Enter the server IP address and optionally , for FTP servers, the port number.
<ip>	Enter the server IP address.
<string>	Enter the path and file name for the backup.
<username>	Enter username to use to log on the backup server.
<passwd>	Enter the password for the username on the backup server. Note: You cannot use <code>\\</code> in passwords.
<ssh-cert>	Enter the SSH certification for the server. This option is only available for backup operations to SCP servers.
[crptpasswd]	Optional password to protect backup content. Leave blank for no password.
<directory>	Enter the path to where the file will be backed up to on the backup server.
[vdlist]	VD name(s), separated by commas.
[force-docker]	Optional flag to stop when the docker backup fails.

Example

This example shows how to backup the FortiAnalyzer unit system settings to a file named `fmg.cfg` on a server at IP address 192.168.1.23 using the admin username, and password 123457.

```
execute backup all-settings ftp 192.168.1.23 fmd.cfg admin 123456
Starting backup all settings in background, please wait.
# Starting transfer the backup file to FTP server...
```

```
Transferred 139.237M of 139.237M in 0:00:00s (178.065M/s)
Backup all settings...Ok.
MD5: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

bootimage

Set the image from which the FortiAnalyzer unit will boot the next time it is restarted.



This command is only available on hardware-based FortiAnalyzer models.

Syntax

```
execute bootimage {primary | secondary}
```

Variable	Description
{primary secondary}	Select to boot from either the primary or secondary partition.

If you do not specify primary or secondary, the command will report whether it last booted from the primary or secondary boot image.

If your FortiAnalyzer unit does not have a secondary image, the bootimage command will inform you that option is not available.

To reboot your FortiAnalyzer unit, use:

```
execute reboot
```

certificate

Use these commands to manage certificates.

certificate ca

Use these commands to list, import, or export CA certificates.

Syntax

To list the CA certificates installed on the FortiAnalyzer unit:

```
execute certificate ca list
```

To export or import CA certificates:

```
execute certificate ca export <cert_name> <tftp_ip>
execute certificate ca import <filename> <tftp_ip> <cert_name>
```

Variable	Description
list	Generate a list of CA certificates on the FortiAnalyzer system.
<export>	Export CA certificate to TFTP server.
<import>	Import CA certificate from a TFTP server.
<cert_name>	Name of the certificate.
<tftp_ip>	IP address of the TFTP server.
<filename>	File name on the TFTP server.

certificate crl

Use this command to import CRL certificate from a TFTP server.

Syntax

```
execute certificate crl import <filename> <tftp_ip> <cert_name>
```

certificate local

Use these commands to list, import, or export local certificates, and to generate a certificate request

Syntax

```
execute certificate local export <cert_name> <tftp_ip>
execute certificate local import <filename> <tftp_ip> <cert_name>
execute certificate local import-pkcs12 {ftp | scp | sftp} <ip:port> <filename>
    <username> <password> <password> <name>
execute certificate local generate <certificate-name-string> <subject> <number>
    [<optional_information>]
execute certificate local list
```

Variable	Description
export <cert_name> <tftp_ip>	Export a certificate or request to a TFTP server. <ul style="list-style-type: none"> cert_name - Name of the certificate. tftp_ip - IP address of the TFTP server.
import <filename> <tftp_ip> <cert_name>	Import a signed certificate from a TFTP server.

Variable	Description
import-pkcs12 {ftp scp sftp} <ip:port> <filename> <username> <password> <password> <name>	Import a certificate and private key from a PKCS#12 file. <ul style="list-style-type: none"> ftp, scp, sftp - The type of server the file will be imported from. ip:port - The server IP address and, optional, the port number. filename - The path and file name on the server. username - The user name on the server. password - The user password. password - The file password. name - The certificate name.
generate <certificate-name_str> <number> <subject> [<optional_ information>]	Generate a certificate request. <ul style="list-style-type: none"> certificate-name-string - Enter a name for the certificate. The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and _. Other special characters and spaces are not allowed. number - The size, in bits, of the encryption key, 512, 1024, 1536, or 2048. subject - Enter one of the following pieces of information to identify the FortiAnalyzer unit being certified: <ul style="list-style-type: none"> The FortiAnalyzer unit IP address The fully qualified domain name of the FortiAnalyzer unit An email address that identifies the FortiAnalyzer unit An IP address or domain name is preferable to an email address. optional_information - Enter optional_information as required to further identify the unit. See Optional information variables on page 172 for more information.
list	Generate a list of CA certificates and requests that are on the FortiAnalyzer system.

Optional information variables

You must enter the optional variables in the order that they are listed in the table. To enter any optional variable you must enter all of the variables that come before it in the list.

For example, to enter the `organization_name_str`, you must first enter the `country_code_str`, `state_name_str`, and `city_name_str`.

While entering optional variables, you can type ? for help on the next required variable.

Variable	Description
<country_code_str>	Enter the two-character country code.
<state_name_str>	Enter the name of the state or province where the FortiAnalyzer unit is located.
<city_name_str>	Enter the name of the city, or town, where the person or organization certifying the FortiAnalyzer unit resides.
<organization-name_str>	Enter the name of the organization that is requesting the certificate for the FortiAnalyzer unit.

Variable	Description
<organization-unit_name_str>	Enter a name that identifies the department or unit within the organization that is requesting the certificate for the FortiAnalyzer unit.
<email_address_str>	Enter a contact email address for the FortiAnalyzer unit.

certificate remote

Use these commands to list, import, or export remote certificates.

Syntax

To list the remote certificates installed on the FortiAnalyzer unit:

```
execute certificate remote list
```

To export or import remote certificates:

```
execute certificate remote {<export>|<import>} <cert_name> <tftp_ip>
```

Variable	Description
list	Generate a list of remote certificates on the FortiAnalyzer system.
<export>	Export the certificate to TFTP server.
<import>	Import the certificate from a TFTP server.
<cert_name>	Name of the certificate.
<tftp_ip>	IP address of the TFTP server.

console

console baudrate

Use this command to get or set the console baudrate.

Syntax

```
execute console baudrate [9600 | 19200 | 38400 | 57600 | 115200]
```

If you do not specify a baudrate, the command returns the current baudrate.

Setting the baudrate will disconnect your console session.

Example

Get the baudrate:

```
execute console baudrate
```

The response is displayed:

```
current baud rate is: 9600
```

Set the baudrate to 19200:

```
execute console baudrate 19200
```

date

Get or set the FortiAnalyzer system date.

Syntax

```
execute date [<date_str>]
```

where

`date_str` has the form `mm/dd/yyyy`

- `mm` is the month and can be 1 to 12
- `dd` is the day of the month and can be 1 to 31
- `yyyy` is the year and can be 2001 to 2037

If you do not specify a date, the command returns the current system date.

Dates entered will be validated - `mm` and `dd` require one or two digits, and `yyyy` requires four digits. Entering fewer digits will result in an error.

Example

This example sets the date to 29 September 2020:

```
execute date 9/29/2020
```

device

Use this command to change a device password, serial number, or user when changing devices due to a hardware issue.

Syntax

```
execute device replace pw <device_name> <password>  
execute device replace sn <device_name> <serial_number>
```

```
execute device replace user <device_name> <user>
```

Variable	Description
pw	Replace the device password.
sn	Replace the device serial number.
user	Replace the device user.
<device_name>	The name of the device.
<password>	The new password for the new device.
<serial_number>	The new serial number for the new device, for example: FWF40C391XXX0062.
<user>	The new user for the new device.

Example

```
execute device replace pw FGT600C2805030002
This operation will clear the password of the device.
Do you want to continue? (y/n)y
```

erase-disk

Overwrite the flash (boot device) with random data a specified number of times. When you run this command, you will be prompted to confirm the request.



Executing this command will overwrite all information on the FortiAnalyzer system's flash drive. The FortiAnalyzer system will no longer be able to boot up.

Syntax

```
execute erase-disk flash <erase-times>
```

Variable	Description
<erase-times>	Number of times to overwrite the flash with random data (1 - 35, default = 1).

factory-license

Use this command to enter a factory license key. This command is hidden.

Syntax

```
execute factory-license <key>
```

Variable	Description
<key>	The factory license key.

fmupdate

Import or export packages using the FTP, SCP, or TFTP servers.

Syntax

```
execute fmupdate {ftp | scp | tftp} import <type> <filename> <server> <port> <directory>
    <username> <password>
execute fmupdate {ftp | scp | tftp} export <type> <filename> <server> <port> <directory>
    <username> <password>
execute fmupdate {ftp | scp | tftp} fds-export <objid> <filename> <server> <directory>
    <username> <password>
execute fmupdate fgdb-db-merge {as | av | av2 | fq | iot | wf}
```

Variables	Description
{ftp scp tftp}	Select the file transfer protocol to use: ftp, scp, or tftp.
fds-export	Export the AV-IPS package to the FTP server.
fgdb-db-merge {as av av2 fq iot wf}	Merge FortiGuard database immediately. Select the database type.
<type>	Select the package type to export or import: <ul style="list-style-type: none"> import: <ul style="list-style-type: none"> package = fcp package license = license package custom-url = customized URL database export: <ul style="list-style-type: none"> license = license package license-xml = license info. in xml custom-url = customized URL database
<filename>	Update manager packet file name on the server or host.
<objid>	Enter the object ID (use '-' as a separator).
<server>	Enter the FQDN or the IP address of the server.
<port>	Only available when the file transfer protocol is scp. Enter the port to connect to on the remote SCP host (1 - 65535).

Variables	Description
<directory>	Enter the name of the directory of the file to download from the FTP server or SCP host. If the directory name has spaces, use quotes instead.
<username>	Enter the username to log into the FTP server or SCP host
<password>	Enter the password to log into the FTP server or SCP host

format

Format the hard disk on the FortiAnalyzer system. You can select to perform a secure (deep-erase) format which overwrites the hard disk with random data. You can also specify the number of time to erase the disks.

Syntax

```
execute format <disk | disk-ext3 | disk-ext4> <RAID level> deep-erase <erase-times>
```

When you run this command, you will be prompted to confirm the request.



Executing this command will erase all device settings/images, databases, and log data on the FortiAnalyzer system's hard drive. The FortiAnalyzer device's IP address, and routing information will be preserved.

Variable	Description
<disk disk-ext3 disk-ext4>	Select to format the hard disk or format the hard disk with ext3 or ext4 file system.
deep-erase	Overwrite the hard disk with random data. Selecting this option will take longer than a standard format.
<erase-times>	Number of times to overwrite the hard disk with random data (1 - 35, default = 1).
<RAID level>	Enter the RAID level to be set on the device. This option is only available on FortiAnalyzer models that support RAID. Enter * to show available RAID levels.

fortirecorder

This command allows you to delete all FortiRecorder videos.

It is only available on hardware devices that support FortiRecorder.

Syntax

```
execute fortirecorder camera-password-reset <vendor-name> <model-name> <ip-addr> <mac-addr>
execute fortirecorder delete-video <camera names>
```

Variable	Description
camera-password-reset	Reset the camera password.
delete-video	Delete all videos.
<camera names>	The names of the cameras whose videos will be deleted, separated by commas with no spaces.
<ip-addr>	Enter the IP address.
<mac-addr>	Enter the MAC address.
<model-name>	Enter the model name.
<vendor-name>	Enter the vendor name.

iotop

Use this command to display system processes input/output usage information.

Syntax

```
execute iotop <parameter> <parameter> <parameter> <parameter> <parameter> <parameter>
<parameter> <parameter>
```

Parameter	Description
--version	Show the program's version number and exit.
-h, --help	Show this help message and exit.
-o, --only	Only show processes or threads that are actually doing I/O.
-b, --batch	Non-interactive mode.
-n NUM, --iter=NUM	The number of iterations before ending (default = infinite).
-d SEC, --delay=SEC	The delay between iterations, in seconds (default = 1).
-p PID, --pid=PID	The processes/threads to monitor (default = all).
-u USER, --user=USER	The users to monitor (default = all).
-P, --processes	Only show processes, not all threads.
-a, --accumulated	Show the accumulated I/O instead of bandwidth.

Parameter	Description
-k, --kilobytes	Use kilobytes instead of a human friendly unit.
-t, --time	Add a timestamp on each line (implies --batch).
-q, --quiet	Suppress some lines of header (implies --batch).

iotps

Use this command to list system processes sorted by their read/write system call rate.

Syntax

```
execute iotps <parameter> <parameter> <parameter> <parameter> <parameter> <parameter>
```

Variable	Description
<parameter>	Parameters: <ul style="list-style-type: none"> • -r • -w • -e • -t [intv]

log

Use the following commands to manage device logs:

log adom disk-quota	log dlp-files clear
log device disk-quota	log import
log device logstore	log ips-pkt clear
log device permissions	log quarantine-files clear
log device vdom	log storage-warning

log adom disk-quota

Set the ADOM disk quota.

Syntax

```
execute log adom disk-quota <adom_name> <value>
```

Variable	Description
<adom_name>	Enter the ADOM name, or enter <code>All</code> for all ADOMs.
<value>	Enter the disk quota value in megabytes.

log device disk-quota

Set the log device disk quota.

Syntax

```
execute log device disk-quota <device_id> <value>
```

Variable	Description
<device_id>	Enter the log device ID, or enter <code>All</code> for all devices.
<value>	Enter the disk quota value in megabytes.

log device logstore

Use this command to view and edit log storage information.

Syntax

```
execute log device logstore clear <device_id>
execute log device logstore list
```

Variable	Description
clear <device_id>	Remove leftover log directory.
list	List log storage directories.

log device permissions

Use this command to view and set log device permissions.

Syntax

```
execute log device permissions <device_id> <permission> {enable | disable}
```

Variable	Description
<device_id>	Enter the log device ID, or enter <code>All</code> for all devices. Example: <code>FWF40C3911000061</code>
<permission>	The following options are available: <ul style="list-style-type: none"> • <code>all</code>: All permissions • <code>logs</code>: Log permission • <code>content</code>: Content permission • <code>quar</code>: Quarantine permission • <code>ips</code>: IPS permission.
{enable disable}	Enable/disable permissions.

log device vdom

Use this command to add, delete, or list VDOMs.

Syntax

```
execute log device vdom add <Device Name> <ADOM> <VDOM>
execute log device vdom delete <Device Name> <VDOM>
execute log device vdom delete-by-id <Device Name> <index>
execute log device vdom list <Device Name>
```

Variable	Description
add <Device Name> <ADOM> <VDOM>	Add a new VDOM to a device with the device name, the ADOM that contains the device, and the name of the new VDOM.
delete <Device Name> <VDOM>	Delete a VDOM from a device.
delete-by-id <Device Name> <index>	Delete a VDOM from a device by its index number.
list <Device Name>	List all the VDOMs on a device.

log dlp-files clear

Use this command to clear DLP log files on a specific log device.

Syntax

```
execute log dlp-files clear <device_name> <archive type>
```

Variable	Description
<device_name>	Enter the device name.
<archive type>	Enter the device archive type: <code>all</code> , <code>email</code> , <code>im</code> , <code>ftp</code> , <code>http</code> , or <code>mms</code> .

log import

Use this command to import log files from another device and replace the device ID on imported logs.

Syntax

```
execute log import <service> <ip:port> <user-name> <password> <file-name> <device-id>
```

Variable	Description
<service>	Enter the transfer protocol one of: ftp, sftp, scp, or tftp.
<ip:port>	Server IP address or host name. Port is optional.
<user-name>	Enter the username.
<password>	Enter the password or '-' for no password. The <password> field is not required when <service> is tftp.
<file-name>	The file name (e.g. dir/fgt.alog.log) or directory name (e.g. dir/subdir/).
<device-id>	Replace the device ID on imported logs. Enter a device serial number of one of your log devices.

log ips-pkt clear

Use this command to clear IPS packet logs on a specific log device.

Syntax

```
execute log ips-pkt clear <device_name>
```

Variable	Description
<device_name>	Enter the device name.

log quarantine-files clear

Use this command to clear quarantine log files on a specific log device.

Syntax

```
execute log quarantine-files clear <device_name>
```

Variable	Description
<device_name>	Enter the device name.

log storage-warning

Reset the licensed VM storage size warning

Syntax

```
execute log storage-warning reset
```

log-aggregation

Immediately upload the log to the server.

Syntax

```
execute log-aggregation <id>
```

Variable	Description
<id>	The client ID, or <code>all</code> for all clients.

log-fetch

Use the following commands to fetch logs.

log-fetch client

Use these commands to manage client sessions.

Syntax

```
execute log-fetch client cancel <profile name>
execute log-fetch client list <profile name>
execute log-fetch client pause <profile name>
execute log-fetch client resume <profile name>
execute log-fetch client run <profile name>
execute log-fetch client view <profile name>
```

Variable	Description
cancel <profile name>	Cancel one session.
list <profile name>	List all sessions.

Variable	Description
pause <profile name>	Pause one session.
resume <profile name>	Resume one session.
run <profile name>	Start a new session.
view <profile name>	View the session status.

log-fetch server

Use this command to manager the log fetching server.

Syntax

```
execute log-fetch server approve <session id>
execute log-fetch server cancel <session id>
execute log-fetch server deny <session id>
execute log-fetch server list
execute log-fetch server pause <session id>
execute log-fetch server resume <session id>
execute log-fetch server view <session id>
```

Variable	Description
approve <session id>	Approve a session.
cancel <session id>	Pause and clear one session or all sessions.
deny <session id>	Deny a session.
list	List all sessions.
pause <session id>	Pause a session.
resume <session id>	Resume a session.
view <session id>	View the session.

log-integrity

Query the log file's MD5 checksum and timestamp.

Syntax

```
execute log-integrity <device_name> <vdom name> <log_name>
```


Variable	Description
<device_name>	The name of the log device.
<vdom name>	The VDOM name.
<log_name>	The log file name.

lvm

With Logical Volume Manager (LVM), a FortiAnalyzer VM device can have up to fifteen total log disks added to an instance. More space can be added by adding another disk and running the LVM extend command.



This command is only available on FortiAnalyzer VM models.



You can use the `execute format disk` command to start the LVM. See [format](#) on page 177.

Syntax

```
execute lvm extend
execute lvm info
```

Variable	Description
extend	Extend the LVM logical volume.
info	Get system LVM information.

migrate

Use this command to migrate all backup settings from the FTP, SCP, or SFTP server to the new FortiAnalyzer serial number or FortiAnalyzer HA cluster serial numbers.

This command also allows migrating to the fabric ADOM from a non-fabric ADOM.

Syntax

```
execute migrate all-settings {ftp | scp | sftp} <ip:port> <string> <username> <password>
    <ssh-cert> [<crptpasswd>]
execute migrate fabric <adom name>
execute migrate serial-number-list <serial-number-list>
```

Variable	Description
{ftp scp sftp}	Enter the server type: ftp, scp, or sftp.
<ip:port>	Enter the server IP address and optionally, for FTP servers, the port number.
<string>	Enter the path and file name for the backup.
<username>	Enter username to use to log on the backup server.
<password>	Enter the password for the username on the backup server.
<ssh-cert>	Enter the SSH certification for the server. This option is only available for backup operations to SCP servers.
[<crptpasswd>]	Optional password to protect backup content. Use <code>any</code> for no password.
<adom name>	Enter names of the ADOM(s) separated by commas.
<serial-number-list>	Enter the serial number. The serial number list is separated by commas, e.g., <code>sno_1, sno_2</code> .

ping

Send an ICMP echo request (ping) to test the network connection between the FortiAnalyzer system and another network device.

Syntax

```
execute ping <ip | hostname>
```

Variable	Description
<ip hostname>	IPv4 address or DNS resolvable hostname of network device to contact.

Example

This example shows how to ping a host with the IPv4 address 192.168.1.23:

```
execute ping 192.168.1.23
```

ping6

Send an ICMP echo request (ping) to test the network connection between the FortiAnalyzer system and another network device.

Syntax

```
execute ping6 <ip | hostname>
```

Variable	Description
<ip hostname>	Enter the IPv6 address or DNS resolvable hostname of network device to contact.

Example

This example shows how to ping a host with the IPv6 address 8001:0DB8:AC10:FE01:0:0:0:0:

```
execute ping6 8001:0DB8:AC10:FE01:0:0:0:0:
```

raid

This command allows you to add and delete RAID disks.



This command is only available on hardware-based FortiAnalyzer models that support RAID.

Syntax

```
execute raid add-disk <disk index>  
execute raid delete-disk <disk index>
```

Variable	Description
add-disk <disk index>	Add a disk and give it an index number.
delete-disk <disk index>	Delete the specified disk.

reboot

Restart the FortiAnalyzer system. This command will disconnect all sessions on the FortiAnalyzer system.

Syntax

```
execute reboot
```

remove

Use this command to remove all GUI data cache, all custom settings in Logview, all reports for a specific device, resync files, security fabric from a specific ADOM, and all endpoints and end user related information from files, tables, and memory.

Syntax

```
execute remove endpoints-endusers
execute remove gui-data-cache
execute remove gui-logview-settings
execute remove reports [device-id]
execute remove resync
execute remove security-fabric <adom-name> <security-fabric-name>
```

Variable	Description
<device-id>	The device identifier for the device that all reports are being removed from.
<adom-name>	The ADOM that contains the security fabric that is being removed.
<security-fabric-name>	The security fabric that is being removed.

Example

```
execute remove gui-logview-settings
This operation will Remove all custom settings in GUI LogView and reset to default for
all users.
Do you want to continue? (y/n)y

Remove all custom settings in GUI LogView ...
Done! Reset all settings in GUI LogView to default.
```

reset

Use these commands to reset the FortiAnalyzer unit. These commands will disconnect all sessions and restart the FortiAnalyzer unit.

Syntax

```
execute reset adom-settings <adom> <version> <mr> <ostype>
execute reset all-except-ip
execute reset all-settings
execute reset all-shutdown
```

Variable	Description
adom-settings <adom> <version> <mr> <ostype>	Reset an ADOM's settings. <ul style="list-style-type: none"> • <adom>: The ADOM name. • <version>: The ADOM version. For example, 5 for 5.x releases. • <mr>: The major release number. • <ostype>: Supported OS type. For example, 18 for FortiDeceptor.
all-except-ip	Reset all settings except the current IP address and route information.
all-settings	Reset to factory default settings.
all-shutdown	Reset all settings and shutdown.

restore

Use this command to:

- restore the configuration or database from a file
- change the FortiAnalyzer unit image
- Restore device logs, DLP archives, and reports from specified servers.

This command will disconnect all sessions and restart the FortiAnalyzer unit.

Syntax

```
execute restore all-settings {ftp | sftp} <ip:port> <filename> <username> <password>
    [<crptpasswd>] [option1+option2+...]
execute restore all-settings scp <ip> <filename> <username> <ssh-cert> [<crptpasswd>]
    [option1+option2+...]
execute restore image {ftp | scp | sftp} <filepath> <ip:port> <username> <password>
execute restore image tftp <string> <ip>
execute restore logs <device name(s)> {ftp | scp | sftp} <ip> <username> <password>
    <directory> [vdlist]
execute restore logs-only <device name(s)> {ftp | scp | sftp} <ip> <username> <password>
    <directory> [vdlist]
execute restore reports <report name(s)> {ftp | scp | sftp} <ip> <username> <password>
    <directory> [vdlist]
execute restore reports-config {<adom_name> | all} {ftp | scp | sftp} <ip> <username>
    <password> <directory> [full]
```

Variable	Description
all-settings	Restore all FortiAnalyzer settings from a file on a FTP, SFTP, or SCP server. The new settings replace the existing settings, including administrator accounts and passwords.
image	Upload a firmware image from a(an) FTP/SCP/SFTP/TFTP server to the FortiAnalyzer unit. The FortiAnalyzer unit reboots, loading the new firmware.
logs	Restore device logs and DLP archives from a specified server.

Variable	Description
logs-only	Restore device logs from a specified server.
reports	Restore reports from a specified server.
reports-config	Restore report configurations to a specified server.
ftp	Restore from an FTP server.
sftp	Restore from a SFTP server.
scp	Restore from an SCP server.
<ip:port>	Enter the IP address of the server to get the file from and optionally , for FTP servers, the port number.
<ip>	Enter the server IP address.
<device names>	Device name or names, separated by commas, or <code>all</code> for all devices. Example: <code>FWF40C3911000061</code>
<report name(s)>	Restore specific reports (separated by commas), <code>all</code> for all reports, or reports with names containing given pattern. A '?' matches any single character. A '*' matches any string, including the empty string, e.g.: <ul style="list-style-type: none"> <code>foo</code>: for exact match <code>*foo</code>: for report names ending with foo <code>foo*</code>: for report names starting with foo <code>*foo*</code>: for report names containing foo substring.
{<adom_name> all}	Select to backup a specific ADOM or all ADOMs.
<filename>	Enter the file to get from the server. You can enter a path with the filename, if required.
<filepath>	Enter the file path on the FTP server.
<username>	The username to log on to the server. This option is not available for restore operations from TFTP servers.
<password>	Enter the password, or – if there is no password.
<ssh-cert>	Enter the SSH certificate used for user authentication on the SCP server.
[<crtpasswd>]	Optional password to protect backup content. Use <code>any</code> for no password.
[option1+option2+...]	Enter <code>keepbasic</code> to retain IP and routing information on the original unit.
<directory>	Enter the directory.
[full]	Reports configuration full restoration.

Example

This example shows how to upload a configuration file from a FTP server to the FortiAnalyzer unit. The name of the configuration file on the FTP server is `backupconfig`. The IP address of the FTP server is 192.168.1.23. The user is

admin with a password of mypassword. The configuration file is located in the /usr/local/backups/ directory on the FTP server.

```
execute restore all-settings ftp 192.168.1.23 /usr/local/backups/backupconfig admin  
mypassword
```

sensor

This command lists sensors and readings.



This command is only available on hardware-based FortiAnalyzer models.

Syntax

```
execute sensor detail  
execute sensor list
```

Variable	Description
detail	List detailed sensors and readings.
list	List sensors and readings.

shutdown

Shut down the FortiAnalyzer system. This command will disconnect all sessions.

Syntax

```
execute shutdown
```

sql-local

Use this command to remove the SQL database and logs from the FortiAnalyzer system and to rebuild the database and devices.



When rebuilding the SQL database, new logs will not be available until the rebuild is complete. The time required to rebuild the database is dependent on the size of the database. Please plan a maintenance window to complete the database rebuild. You can use the `diagnose sql status rebuild-db` command to display the SQL log database rebuild status.

The following features will not be available until after the SQL database rebuild has completed: FortiView, Log View, Event Management, and Reports.

Syntax

```
execute sql-local rebuild-adom <adom> ... <adom>
execute sql-local rebuild-db
execute sql-local rebuild-index <adom> <start-time> <end-time>
execute sql-local rebuild-skipidx <adom> <start-time> <end-time>
```

Variable	Description
rebuild-adom	Rebuild log SQL database from log data for particular ADOMs.
rebuild-db	Rebuild entire log SQL database from log data. This operation will remove the SQL database and rebuild from log data. It will also reboot the device.
rebuild-index	Rebuild indexes for an ADOM.
rebuild-skipidx	Rebuild skip-indexes.
<adom>	The ADOM name. Multiple ADOM names can be entered when rebuilding ADOMs.
<start-time>	Enter the start time (timestamp or <yyyy-mm-dd hh:mm:ss>).
<end-time>	Enter the end time (timestamp or <yyyy-mm-dd hh:mm:ss>).
<log type>	Enter the log type from available log types, for example: <code>emailfilter</code>

sql-query-dataset

Use this command to execute a SQL dataset against the FortiAnalyzer system.

Syntax

```
execute sql-query-dataset <adom> <dataset-name> <device/group name> <faz/dev> <start-time> <end-time>
```

Variable	Description
<adom_name>	Enter the ADOM name.
<dataset-name>	Enter the SQL dataset name.

Variable	Description
<device/group name>	Enter the name of the device or device group.
<faz/dev>	Enter the reference time: FortiAnalyzer time or device time.
<start-time>	Enter the log start time (timestamp or <yyyy-mm-dd hh:mm:ss>).
<end-time>	Enter the log end time (timestamp or <yyyy-mm-dd hh:mm:ss>).

sql-query-generic

Use this command to execute a SQL statement against the FortiAnalyzer system.

Syntax

```
execute sql-query-generic <string>
```

Variable	Description
<string>	Specify the SQL statement to be executed.

sql-report

Use these commands to import and display language translation and font files, and run a SQL report schedule once against the FortiAnalyzer system.

Syntax

```
execute sql-report delete-font <font-name>
execute sql-report delete-lang <language-name>
execute sql-report delete-template adom-installed <adom> <language> [title]
execute sql-report delete-template device-default <dev-type> <language> [title]
execute sql-report export-lang <language-name> <service> <ip> <argument 1> <argument 2>
    <argument 3>
execute sql-report export-template adom-installed <adom> <service> <ip> <user> <password>
    <file name> [language] [title]
execute sql-report export-template device-default <dev-type> <service> <ip> <user>
    <password> <file name> [language] [title]
execute sql-report hcache-build <adom> <schedule-name> <start-time> <end-time>
execute sql-report hcache-check <adom> <schedule-name> <start-time> <end-time>
execute sql-report import-font <service> <ip> <argument 1> <argument 2> <argument 3>
execute sql-report import-lang <language-name> <service> <ip> <argument 1> <argument 2>
    <argument 3>
execute sql-report import-template <devtype> <service> <ip> <user> <password> <file name>
execute sql-report install-template <adom> <language> <service> <ip> <user> <password>
    <file name>
execute sql-report list <adom> [days-range] [layout-name]
```

```

execute sql-report list-fonts
execute sql-report list-lang [language]
execute sql-report list-schedule <adom> [sched-only | autocache-only | detail] [detail]
execute sql-report list-template adom-installed <adom> [language]
execute sql-report list-template device-default <dev-type> [language]
execute sql-report run <adom> <schedule-name> <start-time> <end-time>
execute sql-report view <data-type> <adom> <report-name>

```

Variable	Description
delete-font	Delete one font.
delete-lang	Delete one language translation file.
delete-template	Delete templates. <ul style="list-style-type: none"> • adom-installed - Delete report templates installed in ADOM. • device-default - Delete device type default report templates.
export-lang	Export a user-defined language translation file.
export-template	Export report templates. <ul style="list-style-type: none"> • adom-installed - Export ADOM report templates to file. • device-default - Export device type default report templates to file.
hcache-build	Build report hcache.
hcache-check	Check report hcache.
import-font	Import one font.
import-lang	Import a user-defined language translation file.
import-template	Import per device type template from a configuration file.
install-template	Install specific language templates to an ADOM.
list	List recent generated reports.
list-fonts	List all imported fonts.
list-lang	Display all supported language translation files.
list-schedule	List report schedule and autocache information.
list-template	List templates. <ul style="list-style-type: none"> • adom-installed - Display report templates installed in ADOM. • device-default - Display device type default report templates.
run	Run a report once.
view	View report data.
<adom>	Specify the ADOM name.
<font-name>	The name of a font.
<dev-type>	Enter the device type abbreviation: <ul style="list-style-type: none"> • FGT - FortiGate • FAZ - FortiAnalyzer

Variable	Description
	<ul style="list-style-type: none"> • FMG - FortiManager • FCT - FortiClient • FML - FortiMail • FWB - FortiWeb • FCH - FortiCache • FSA - FortiSandbox • FDD - FortiDDoS • FAC - FortiAuthenticator • FPX - FortiProxy
<language-name>	<p>Enter the language name to import, export, or delete a language translation file, or select one of the following options:</p> <ul style="list-style-type: none"> • English • French • Japanese • Korean • Portuguese • Simplified_Chinese • Spanish • Traditional_Chinese
<service>	<p>Enter the transfer protocol: ftp, sftp, scp, or tftp. TFTP is not available for all commands.</p>
<ip>	Enter the server IP address.
<argument 1>	For FTP, SFTP, or SCP, type a user name. For TFTP, enter a file name.
<argument 2>	For FTP, SFTP, or SCP, type a password or '-'. For TFTP, press <enter>.
<argument 3>	Enter a file name and press <enter>.
<user>	Enter a user name for the remote server.
<password>	Enter the password, or -, for the remote server user.
<file name>	Enter the name of the file.
<data-type>	The data type to view: report-data or report-log.
<report-name>	The name of the report to view.
<schedule-name>	Select one of the available report schedule names.
<start-time>	The start date and time of the report schedule, in the format: "HH:MM yyyy/mm/dd"
<end-time>	The enddate and time of the report schedule, in the format: "HH:MM yyyy/mm/dd"
[days-range]	The recent n days to list reports, from 1 to 99.
[layout-name]	One of the available SQL report layout names.
[language]	<p>Enter the language abbreviation:</p> <ul style="list-style-type: none"> • en - English • de - German • es - Spanish • ko - Korean • pt - Portuguese • ru - Russian

Variable	Description
	<ul style="list-style-type: none"> • <code>fr</code> - French • <code>it</code> - Italian • <code>ja</code> - Japanese • <code>zh</code> - Simplified Chinese • <code>zh_Hant</code> - Traditional Chinese
<code>[title]</code>	Title of a specific report template.

ssh

Use this command to establish an SSH session with another system.

Syntax

```
execute ssh <destination> <username>
```

Variable	Description
<code><destination></code>	Enter the IP or FQ DNS resolvable hostname of the system you are connecting to.
<code><username></code>	Enter the user name to use to log on to the remote system.

To leave the SSH session type `exit`. To confirm that you are connected or disconnected from the SSH session, verify that the command prompt has changed.

ssh-known-hosts

Use this command to remove known SSH hosts.

Syntax

```
execute ssh-known-hosts remove-all
execute ssh-known-hosts remove-host <host/ip>
```

Variable	Description
<code>remove-all</code>	Remove all known SSH hosts.
<code>remove-host</code>	Remove the specified SSH hosts. <ul style="list-style-type: none"> • <code><host/IP></code> - The hostname or IP address of the SSH host to remove.

tac

Use this command to upload, debug, or remove dangling debug reports older than an hour.

Syntax

```
execute tac cleanup
execute tac report
execute tac upload <service> <ip> <dir> <user name> <password>
```

Variable	Description
<service>	Enter the transfer protocol: <code>ftp</code> , <code>sftp</code> , or <code>scp</code> .
<ip>	Enter the server IP address. For <code>ftp</code> , the port can be specified by adding <code>:port</code> .
<dir>	Enter the directory.
<user name>	Enter the username.
<password>	Enter the password or enter <code>-</code> for no password.

time

Get or set the system time.

Syntax

```
execute time [<time_str>]
```

Variable	Description
[<time_str>]	<p>The time of day, in the form <code>hh:mm:ss</code>.</p> <ul style="list-style-type: none"><code>hh</code> is the hour and can be <code>00</code> to <code>23</code><code>mm</code> is the minutes and can be <code>00</code> to <code>59</code><code>ss</code> is the seconds and can be <code>00</code> to <code>59</code> <p>All parts of the time are required. Single digits are allowed for each of <code>hh</code>, <code>mm</code>, and <code>ss</code>.</p>

If you do not specify a time, the command returns the current system time.

Example

This example sets the system time to `15:31:03`:

```
execute time 15:31:03
```

top

Use this command to view the processes running on the FortiAnalyzer system.

Syntax

```
execute top <parameter> <parameter> ... <parameter>
```

Variable	Description
<parameter>	The following parameters can be used: -hv -bcHiOSs -d secs -n max -u U user -p pid(s) -o field -w [cols]

execute top help menu

Use the following commands when viewing the running processes. Press **h** or **?** for help.

Command	Description
Z,B,E,e	Global: 'Z' colors; 'B' bold; 'E'/'e' summary/task memory scale
l,t,m	Toggle Summary: 'l' load avg; 't' task/cpu stats; 'm' memory info
0,1,2,3,l	Toggle: '0' zeros; '1/2/3' cpus or numa node views; 'l' lrix mode
f,F,X	Fields: 'f'/'F' add/remove/order/sort; 'X' increase fixed-width
L,&,<,> .	Locate: 'L'/'&' find/again; Move sort column: '<'/'>' left/right
R,H,V,J .	Toggle: 'R' Sort; 'H' Threads; 'V' Forest view; 'J' Num justify
c,i,S,j .	Toggle: 'c' Cmd name/line; 'i' Idle; 'S' Time; 'j' Str justify
x,y.	Toggle highlights: 'x' sort field; 'y' running tasks
z,b.	Toggle: 'z' color/mono; 'b' bold/reverse (only if 'x' or 'y')
u,U,o,O .	Filter by: 'u'/'U' effective/any user; 'o'/'O' other criteria
n,#,^O.	Set: 'n'/'#' max tasks displayed; Show: Ctrl+'O' other filter(s)
C,....	Toggle scroll coordinates msg for: up,down,left,right,home,end
k,r	Manipulate tasks: 'k' kill; 'r' renice
d or s	Set update interval
W,Y	Write configuration file 'W'; Inspect other output 'Y'
q or <Esc>	Quit

traceroute

Test the connection between the FortiAnalyzer system and another network device, and display information about the network hops between the device and the FortiAnalyzer system.

Syntax

```
execute traceroute <host>
```

Variable	Description
<host>	Enter the IP address or hostname of network device.

traceroute6

Test the connection between the FortiAnalyzer system and another network device, and display information about the network hops between the device and the FortiAnalyzer system.

Syntax

```
execute traceroute6 <host>
```

Variable	Description
<host>	Enter the IPv6 address or hostname of network device.

diagnose

The `diagnose` commands display diagnostic information that help you to troubleshoot problems.



CLI commands and variables are case sensitive.

auto-delete	fortilogd	report	vpn
cdb	fortirecorder	rtm	
debug	fwmanager	siem	
dlp-archives	ha	sniffer	
docker	hardware	sql	
dvm	incident	svctools	
faz-cdb	license	system	
fmnetwork	log	test	
fmupdate	pm2	upload	

auto-delete

Use this command to view and configure auto-deletion settings.

Syntax

```
diagnose auto-delete dlp-files {delete-now | list}
diagnose auto-delete log-files {delete-now | list}
diagnose auto-delete quar-files {delete-now | list}
diagnose auto-delete report-files {delete-now | list}
```

Variable	Description
dlp-files {delete-now list}	Delete or list DLP files. <ul style="list-style-type: none"><code>delete-now</code>: Delete DLP files right now according to system automatic deletion policy.<code>list</code>: List DLP files according to system automatic deletion policy.
log-files {delete-now list}	Delete or list log files. <ul style="list-style-type: none"><code>delete-now</code>: Delete log files right now according to system automatic

Variable	Description
	deletion policy.
	<ul style="list-style-type: none"> <code>list</code>: List log files according to system automatic deletion policy.
<code>quar-files {delete-now list}</code>	Delete or list quarantine files. <ul style="list-style-type: none"> <code>delete-now</code>: Delete quarantine files right now according to system automatic deletion policy. <code>list</code>: List quarantine files according to system automatic deletion policy.
<code>report-files {delete-now list}</code>	Delete or list report files. <ul style="list-style-type: none"> <code>delete-now</code>: Delete report files right now according to system automatic deletion policy. <code>list</code>: List report files according to system automatic deletion policy.

cdb

Use this command to check the object configuration database integrity, the global policy assignment table, and repair configuration database.

Syntax

```
diagnose cdb check adom-revision [adom] [preview]
diagnose cdb check internet-service-name [adom]
diagnose cdb check update-devinfo logdisk-size [new value] [0 | 1] [model-name]
diagnose cdb check update-devinfo sslvpn-flag <devname>
diagnose cdb upgrade check <action>
diagnose cdb upgrade force-retry <action>
diagnose cdb upgrade log
diagnose cdb upgrade pending-list
diagnose cdb upgrade summary
```

Variable	Description
<code>check adom-revision [adom] [preview]</code>	Check or remove invalid ADOM revision database. Optionally, preview the check before running it.
<code>check internet-service-name [adom]</code>	Check mis-matched internet service name. Optionally, specify the ADOM.
<code>check update-devinfo logdisk-size [new value] [0 1] [model-name]</code>	Update device log disk size. <ul style="list-style-type: none"> <code>new value</code>: Item new value. <code>0 1</code>: update only empty values (default), or always update (1) <code>model-name</code>: Only update on model name (default: all models).
<code>check update-devinfo sslvpn-flag <devname></code>	Upgrade the device SSL-VPN flag on the specified device.
<code>upgrade check <action></code>	Perform a check to see if upgrade and repair is necessary. <ul style="list-style-type: none"> <code>resync-dev-vdoms</code> - Resync and add any missing vdoms from device

Variable	Description
	database to DVM database
upgrade force-retry <action>	Re-run an upgrade that was already performed in previous release.
upgrade log	Display the configuration database upgrade log.
upgrade pending-list	Display the list of upgrades scheduled for the next reboot.
upgrade summary	Display the firmware upgrade summary.

debug

Use the following commands to debug the FortiAnalyzer.

debug application

Use these commands to view or set the debug levels for the FortiAnalyzer applications. All of the debug levels are 0 by default.

Syntax

```

diagnose debug application alertmail <integer>
diagnose debug application apiproxyd <integer>
diagnose debug application archd <integer>
diagnose debug application auth <integer>
diagnose debug application camctld <integer>
diagnose debug application camerad <integer>
diagnose debug application camnotifyd <integer>
diagnose debug application camproxycd <integer>
diagnose debug application camschedd <integer>
diagnose debug application clusterd <integer>
diagnose debug application connector <integer>
diagnose debug application curl <integer>
diagnose debug application discoverd <integer>
diagnose debug application dmapi <integer>
diagnose debug application dns <integer>
diagnose debug application docker <integer>
diagnose debug application dump
diagnose debug application execcmd <integer>
diagnose debug application fabricsyncd <integer>
diagnose debug application fazcfgd <integer>
diagnose debug application fazmaild <integer>
diagnose debug application faznotify <integer>
diagnose debug application fazsvcd <integer>
diagnose debug application fazwatchd <integer>
diagnose debug application fdssvrd <integer>
diagnose debug application fgdlinkd <integer>
diagnose debug application fgdsvr <integer>

```

```

diagnose debug application fgdupd <integer>
diagnose debug application fgfmsd <integer> <deviceName>
diagnose debug application filefwd <integer>
diagnose debug application fileparsed <integer>
diagnose debug application fortilogd <integer>
diagnose debug application fortimanagerws <integer>
diagnose debug application fortimeter <integer>
diagnose debug application gui <integer>
diagnose debug application ha <integer>
diagnose debug application ipsec <integer>
diagnose debug application localmod <integer>
diagnose debug application log-aggregate <integer>
diagnose debug application logd <integer>
diagnose debug application log-fetchd <integer>
diagnose debug application logfiled <integer>
diagnose debug application logfwd <integer>
diagnose debug application lrm <integer>
diagnose debug application oftpd <integer> <IP/deviceSerial/deviceName>
diagnose debug application quotad <integer>
diagnose debug application rptchkd <integer>
diagnose debug application scansched <integer>
diagnose debug application scheduled <integer>
diagnose debug application siemagentd <integer>
diagnose debug application siemdbd <integer>
diagnose debug application snapd <integer>
diagnose debug application sniffer <integer>
diagnose debug application snmpd <integer>
diagnose debug application sql-integration <integer>
diagnose debug application sqllogd <integer>
diagnose debug application sqlplugind <integer> <filter>
diagnose debug application sqlreportd <integer> <filter>
diagnose debug application sqlrptcached <integer>
diagnose debug application ssh <integer>
diagnose debug application sshd <integer>
diagnose debug application storaged <integer>
diagnose debug application syncsched <integer>
diagnose debug application uploadd <integer>
diagnose debug application vmd <integer>

```

Variable	Description
alertmail <integer>	Set the debug level of the alert email daemon.
apiproxyd <integer>	Set the debug level of the API proxy daemon.
archd <integer>	Set the debug level of the archd daemon (0 - 8).
auth <integer>	Set the debug level of the Fortinet authentication module.
camctld <integer>	Set the debug level of the camera control daemon.
camerad <integer>	Set the debug level of the camera daemon.
camnotifyd <integer>	Set the debug level of the camnotify daemon.
camproxyd <integer>	Set the debug level of the camera proxy daemon.
camschedd <integer>	Set the debug level of the camera scheduler daemon.

Variable	Description
clusterd <integer>	Set the debug level of the clusterd daemon.
connector <integer>	Set the debug level of the connector daemon.
curl <integer>	This command is not in use.
discoverd <integer>	Set the debug level of the camera discovery daemon.
dmapd <integer>	Set the debug level of the dmapd daemon.
dns <integer>	Set the debug level of DNS daemon.
docker <integer>	Set the debug level of the Docker daemon.
dump	Dump services.
execmd <integer>	Set the debug level of the execmd daemon.
fabricsyncd <integer>	Set the debug level of the fabricsyncd daemon (0 - 8).
fazcfgd <integer>	Set the debug level of the fazcfgd daemon.
fazmaild <integer>	Set the debug level of the fazmaild daemon.
faznotify <integer>	Set the debug level of the faznotify daemon.
fazsvcd <integer>	Set the debug level of the FAZ server daemon.
fazwatchd <integer>	Set the debug level of the fazwatchd daemon.
fdssvrd <integer>	Set the debug level of the FDS server daemon.
fgdlinkd <integer>	Set the debug level of the FGD server daemon (0 - 8).
fgdsvr <integer>	Set the debug level of the FortiGuard query daemon.
fgdupd <integer>	Set the debug level of the FortiGuard update daemon.
fgfmsd <integer> <deviceName>	Set the debug level of FGFM daemon. Enter a device name to only show messages related to that device. Note: Enter " " to reset. Multiple device names should be separated by commas. For example, Host1, Host2.
filefwd <integer>	Set the debug level of the filefwd daemon.
fileparsed <integer>	Set the debug level of the fileparsed daemon.
fortilogd <integer>	Set the debug level of the fortilogd daemon.
fortimanagerws <integer>	Set the debug level of the FortiAnalyzer Web Service.
fortimeter <integer>	Set the debug level of the FortiMeter daemon.
gui <integer>	Set the debug level of the GUI.
ha <integer>	Set the debug level of HA.
ipsec <integer>	Set the debug level of the IPsec daemon.

Variable	Description
localmod <integer>	Set the debug level of the localmod daemon.
log-aggregate <integer>	Set the debug level of the log aggregate daemon.
logd <integer>	Set the debug level of the log daemon.
log-fetchd <integer>	Set the debug level of the log fetcher daemon.
logfiled <integer>	Set the debug level of the logfiled daemon.
logfwd <integer>	Set the debug level of the logfwd daemon.
lrm <integer>	Set the debug level of the Log and Report Manager.
oftpd <integer> <IP/deviceSerial/deviceName>	Set the debug level of the oftpd daemon. Enter an IPv4 address, device serial number, or device name to only show messages related to that device or IPv4 address. Note: Enter "" to reset.
quotad <integer>	Set the debug level of the quota daemon.
rptchkd <integer>	Set the debug level of the rptchkd daemon.
scansched <integer>	Set the debug level of the scan schedule daemon.
scheduled <integer>	Set the debug level of the schedule task daemon.
siemagentd <integer>	Set the debug level of the siemagentd daemon.
siemdbd <integer>	Set the debug level of the siemdbd daemon.
snapt <integer>	Set the debug level of the snapshot daemon.
sniffer <integer>	Set the debug level of the interface sniffer.
snmpd <integer>	Set the debug level of the SNMP daemon.
sql-integration <integer>	Set the debug level of SQL applications.
sqllogd <integer>	Set the debug level of SQL log daemon.
sqlplugind <integer> <filter>	Set the debug level of the SQL plugin daemon. Set filter for sqlplugind. Note: Enter "" to reset the filter.
sqlreportd <integer> <filter>	Set the debug level (0-8) of the SQL report daemon. Set the filter for sqlreportd. Note: Enter "" to reset the filter. Without <integer> and <filter>, it shows the current debug level and filter of sqlreportd.
sqlrptcached <integer>	Set the debug level of the SQL report caching daemon.
ssh <integer>	Set the debug level of SSH protocol transactions.
sshd <integer>	Set the debug level of the SSH daemon.
stored <integer>	Set the debug level of communication with java clients.
syncsched <integer>	Set the debug level of the syncsched daemon.

Variable	Description
uploadd <integer>	Set the debug level of the upload daemon.
vmd <integer>	Set the debug level for vmd.

Example

This example shows how to set the debug level to 7 for the upload daemon:

```
diagnose debug application uploadd 7
```

debug backup-oldformat-script-logs

Use this command to backup script log files that failed to be upgraded to the FTP server.

Syntax

```
diagnose debug backup-oldformat-script-logs <ip> <string> <username> <password>
```

Variable	Description
<ip>	Enter the FTP server IP address.
<string>	Enter the path/filename to save the log to the FTP server.
<username>	Enter the user name on the FTP server.
<password>	Enter the password associated with the user name.

debug cdbchk

Use these commands to enable or disable CLI CDB check debug output.

Syntax

```
diagnose debug cdbcheck {enable | disable}
```

debug cli

Use this command to set the debug level of CLI.

Syntax

```
diagnose debug cli <integer>
```

Variable	Description
<integer>	Set the debug level of the CLI (0 - 8, default = 3).

debug console

Use this command to enable or disable console debugging.

Syntax

```
diagnose debug console {enable | disable}
```

Variable	Description
{enable disable}	Enable/disable console debugging.

debug coredump

Use this command to manage daemon and process core dumps.

Syntax

```
diagnose debug coredump crash-pid <pid>
diagnose debug coredump delete <daemon>
diagnose debug coredump disable <daemon>
diagnose debug coredump disable-pid <pid>
diagnose debug coredump enable <daemon>
diagnose debug coredump enable-once <daemon>
diagnose debug coredump enable-pid <pid>
diagnose debug coredump list
diagnose debug coredump upload <daemon> <service> <ip> <username> <password> <directory>
```

Variable	Description
crash-pid <pid>	Crash running process for core dump.
delete <daemon>	Delete core dumps for a daemon.
disable <daemon>	Disable core dump for a daemon.
disable-pid <pid>	Disable core dump of running process.
enable <daemon>	Enable core dump for a daemon.
enable-once <daemon>	Enable core dump the next time a daemon starts (one time only).
enable-pid <pid>	Enable core dump of running process.
list	List core dumps.

Variable	Description
upload <daemon> <service> <ip> <username> <password> <directory>	Upload core dumps for a daemon to the specified server.

debug crashlog

Use this command to clear the debug crash log.

Syntax

```
diagnose debug crashlog clear
diagnose debug crashlog read
```

Variable	Description
clear	Clear the crash log.
read	Read the crash log.

debug disable

Use this command to disable debugging.

Syntax

```
diagnose debug disable
```

debug enable

Use this command to enable debugging.

Syntax

```
diagnose debug enable
```

debug gui

Use these commands to enable or disable the GUI debug flag.

Syntax

```
diagnose debug gui {enable | disable}
```


debug info

Use this command to show active debug level settings.

Syntax

```
diagnose debug info
```

debug klog

Use this command to show all kernel logs.

Syntax

```
diagnose debug klog
```

debug library

Use this command to get or set the debug levels for FortiRecorder library settings. It is only available on hardware devices that support FortiRecorder.

Syntax

```
diagnose debug library aidb <integer>
diagnose debug library cambase <integer>
diagnose debug library camctl <integer>
diagnose debug library camnotify <integer>
diagnose debug library flatfiledb <integer>
diagnose debug library http <integer>
diagnose debug library mediafile <integer>
diagnose debug library mediaproc <integer>
diagnose debug library mediaread <integer>
diagnose debug library onvif <integer>
diagnose debug library packetize <integer>
diagnose debug library rtsp <integer>
diagnose debug library sockio <integer>
```

Variable	Description
aidb <integer>	Set the debug level of the aidb library.
cambase <integer>	Set the debug level of the cambase library.
camctl <integer>	Set the debug level of the camctl library.
camnotify <integer>	Set the debug level of the camnotify library.
flatfiledb <integer>	Set the debug level of the flatfiledb library.
http <integer>	Set the debug level of the http library.

Variable	Description
mediafile <integer>	Set the debug level of the mediafile library.
mediaproc <integer>	Set the debug level of the mediaproc library.
mediaread <integer>	Set the debug level of the mediaread library.
onvif <integer>	Set the debug level of the onvif library.
packetize <integer>	Set the debug level of the packetize library.
rtsp <integer>	Set the debug level of the rtsp library.
sockio <integer>	Set the debug level of the sockio library.

Example

This example shows the debug level of the camctl library:

```
diagnose debug library camctl
  Values: 1 - non-PTZ, 2 - PTZ, 4 - Low-level error
camctl debug level: 0
```

debug raw-elog

Use this command to show raw elog.

Syntax

```
diagnose debug raw-elog
```

debug reset

Use this command reset the debug level settings. All debug settings will be reset.

Syntax

```
diagnose debug reset
```

debug service

Use this command to view or set the debug level of various service daemons, and to dump the services.

Syntax

```
diagnose debug service anonymous <integer>
diagnose debug service cdb <integer>
diagnose debug service cmdb <integer>
```

```
diagnose debug service csf <integer>
diagnose debug service dbcach <integer>
diagnose debug service dvmcmd <integer>
diagnose debug service dvmdb <integer>
diagnose debug service dump
diagnose debug service fazcmd <integer>
diagnose debug service fazconf <integer>
diagnose debug service httpd <integer>
diagnose debug service main <integer>
diagnose debug service rpc-auth <integer>
diagnose debug service sys <integer>
diagnose debug service task <integer>
```

Variable	Description
<integer>	The debug level
dump	Dump the services.

The anonymous, dbcach, dump, fazcmd, and rpc-auth commands are only available on hardware devices.

debug sysinfo

Use this command to show system information.

Syntax

```
diagnose debug sysinfo
```

debug sysinfo-log

Use this command to generate one system info log file every two minutes.

Syntax

```
diagnose debug sysinfo-log {on | off}
```

debug sysinfo-log-backup

Use this command to backup all sysinfo log files to an FTP server.

Syntax

```
diagnose debug sysinfo-log-backup <server> <filepath> <user> <password>
```

Variable	Description
<server>	Enter the FTP server IP address.
<filepath>	Enter the path/filename to save the log to the FTP server.
<user>	Enter the user name on the FTP server.
<password>	Enter the password associated with the user name.

debug sysinfo-log-list

Use this command to display system information elogs.

Syntax

```
diagnose debug sysinfo-log-list <integer>
```

Variable	Description
<integer>	Display the last n elogs (default = 10).

debug timestamp

Use this command to enable or disable debug timestamp.

Syntax

```
diagnose debug timestamp {enable | disable}
```

debug vmd

Use this command to show all the VMD (Virtual Machine Daemon) logs.

Syntax

```
diagnose debug vmd
```

debug vminfo

Use this command to show VM license information.



This command is only available on FortiAnalyzer VM models.

Syntax

```
diagnose debug vminfo
```

dlp-archives

Use this command to manage the DLP archives.

Syntax

```
diagnose dlp-archives quar-cache list-all-process
diagnose dlp-archives quar-cache kill-process <pid>
diagnose dlp-archives rebuild-quar-db
diagnose dlp-archives remove
diagnose dlp-archives statistics {show | flush}
diagnose dlp-archives status
diagnose dlp-archives upgrade
diagnose dlp-archives verify-quar-db
```

Variable	Description
quar-cache list-all-process	List all processes that are using the quarantine cache.
quar-cache kill-process <pid>	Kill a process that is using the quarantine cache.
rebuild-quar-db	Rebuild Quarantine Cache DB
remove	Remove all upgrading DLP archives.
statistics {show flush}	Display or flush the quarantined and DLP archived file statistics.
status	Running status.
upgrade	Upgrade the DLP archives.
verify-quar-db	Verify the quarantine cache database. This command is only available on hardware devices.

docker

Use this command to view Docker status, clean up Docker data, and upgrade Docker management extensions.

Syntax

```
diagnose docker cleanup
diagnose docker reset { fortisoar | fsmcollector }
diagnose docker status
diagnose docker upgrade { fortisoar | fsmcollector }
```

Variable	Description
cleanup	Remove unused Docker data.
reset { fortisoar fsmcollector }	Reset a docker. Select to remove a docker volume and restart.
status	Show Docker status.
upgrade { fortisoar fsmcollector }	Upgrade the specified management extension.

Example

```
# diagnose docker status  
  
fortisoar: disabled  
fsmcollector: disabled
```

dvm

Use the following commands for DVM related settings.

dvm adom

Use this command to list ADOMs.

Syntax

```
diagnose dvm adom list  
diagnose dvm adom reset-default-flags  
diagnose dvm adom unlock <adom>
```

Variable	Description
list	List ADOMs, state, product, OS version (OSVER), major release (MR), name, mode, VPN management, and IPS.
reset-default-flags	Reset ADOM default flags.
unlock <adom>	Remove DVM lock by FortiManager.

dvm capability

Use this command to set the DVM capability.

Syntax

```
diagnose dvm capability set {all | standard}
diagnose dvm capability show
```

Variable	Description
set {all standard}	Set the capability to all or standard.
show	Show what the capability is set to.

dvm chassis

Use this command to list chassis and supported chassis models.

Syntax

```
diagnose dvm chassis list
diagnose dvm chassis supported models
```

Variable	Description
list	List chassis.
supported-models	List supported chassis models.

dvm check-integrity

Use this command to check the DVM database integrity.

Syntax

```
diagnose dvm check-integrity
```

dvm csf

Use this command to print the CSF configuration.

Syntax

```
diagnose dvm csf <adom> <category>
```

Variable	Description
<adom>	The ADOM name.
<category>	The category:

Variable	Description
	<ul style="list-style-type: none"> all: Dump all CSF categories group: Dump CSF group intf-role: Dump interface role user-device: Dump user device

dvm dbstatus

Use this command to print the database status.

Syntax

```
diagnose dvm dbstatus
```

dvm debug

Use this command to enable or disable debug channels, and show debug message related to DVM.

Syntax

```
diagnose dvm debug {enable | disable} <channel> <channel> <channel> ... <channel>
diagnose dvm debug trace [filter]
```

Variable	Description
{enable disable}	Enable/disable debug channels.
trace	Show the DVM debug message.
<channel>	The following channels are available: all, dvm_db, dvm_dev, shelfmgr, ipmi, lib, dvmcmd, dvmcore, gui, and monitor.
[filter]	The following filters are available: all, dvm_db, dvm_dev, shelfmgr, ipmi, lib, dvmcmd, dvmcore, gui, and monitor.

dvm device

Use this command to list devices or objects referencing a device.

Syntax

```
diagnose dvm device delete <adom> <device>
diagnose dvm device dynobj <device>
diagnose dvm device list <device> <vdom>
diagnose dvm device monitor <device> <api>
diagnose dvm device object-reference <device> <vdom> <category> <object>
```


Variable	Description
delete <adom> <device>	Delete a device in a specific ADOM.
dynobj <device>	List dynamic objects on this device.
list <device> <vdom>	List devices. Optionally, enter a device or VDOM name.
monitor <device> <api>	JSON API for device monitor. Specify the device name and the monitor API name.
object-reference <device> <vdom> <category> <object>	List object reference. Specify the device name, VDOM, category (or <i>all</i> for all categories), and object.

dvm device-tree-update

Use this command to enable or disable device tree automatic updates.

Syntax

```
diagnose dvm device-tree-update {enable | disable}
```

Variable	Description
{enable disable}	Enable/disable device tree automatic updates.

dvm extender

Use these commands to list FortiExtender devices, synchronize FortiExtender data via JSON, and perform other actions.

Syntax

```
diagnose dvm extender copy-data-to-device <device>
diagnose dvm extender import-profile <device> <vdom> <name>
diagnose dvm extender import-template <device> <extender id>
diagnose dvm extender list [devname]
diagnose dvm extender reset-adom <adom> [clear-only] [skip-restart]
diagnose dvm extender set-template <device> <extender id> <template>
diagnose dvm extender sync-extender-data <devname> [savedb] [syncadom] [task]
```

Variable	Description
copy-data-to-device <device>	Copy extender data (data plan and SIM profile) to the device. Enter the device name.
import-profile <device> <vdom> <name>	Import extender profile to the ADOM. Enter the device name or ID, VDOM, and profile name.

Variable	Description
import-template <device> <extender id>	Import dataplan and SIM profile to the ADOM template. Enter the device name or ID, and the extender ID.
list [device]	List FortiExtender devices, or those connected to a specific device.
reset-adom <adom> [clear-only] [skip-restart]	Reset all extender data in the ADOM: <ul style="list-style-type: none">• adom: Enter 121 for FortiCarrier, 147 for FortiFirewall, 151 for Unmanaged_Devices, and 3 for root Optionally, use the following variables: <ul style="list-style-type: none">• clear-only: Do not sync extender data to the ADOM• skip-restart: Do not restart FortiManager after the operation
set-template <device> <extender id> <template>	Set template to the extender modem. Enter the device name or ID, extender ID, and template.
sync-extender-data <devname> [savedb] [syncadom] [task]	Synchronize FortiExtender data by JSON. Optionally: save the data to the database, synchronize the ADOM, and/or create a task.

dvm fap

Use this command to list the FortiAP devices connected to a device.

Syntax

```
diagnose dvm fap list <devname>
```

Variable	Description
<devname>	The name of the device.

dvm fsw

Use this command to list the FortiSwitch devices connected to a device.

Syntax

```
diagnose dvm fsw list <devname>
```

Variable	Description
<devname>	The name of the device.

dvm group

Use this command to list groups.

Syntax

```
diagnose dvm group list
```

Variable	Description
list	List groups.

dvm lock

Use this command to print the DVM lock states.

Syntax

```
diagnose dvm lock
```

dvm proc

Use this command to list DVM process (dvmcmd) information.

Syntax

```
diagnose dvm proc list
```

dvm remove

Use this command to remove unused autoupdate debug log files or all unused IPS package files.

Syntax

```
diagnose dvm remove autoupdate-log <device oid>  
diagnose dvm remove unused-ips-packages
```

Variable	Description
autoupdate-log <device oid>	Remove autoupdate debug log files. Enter the device OID.
unused-ips-packages	Remove all unused IPS package files.

dvm supported-platforms

Use this command to list supported platforms.

Syntax

```
diagnose dvm supported-platforms fimg-list
diagnose dvm supported-platforms fortiswitch [<adom>]
diagnose dvm supported-platforms list <detail>
diagnose dvm supported-platforms mr-list
```

Variable	Description
fimg-list	List supported platforms by fimg ID.
fortiswitch [<adom>]	List supported platforms in FortiSwitch manager. Optionally, enter the ADOM name.
list <detail>	List supported platforms by device type. Enter <i>detail</i> to show details with syntax support.
mr-list	List supported platforms by major release.

dvm task

Use this command to repair or reset the task database.

Syntax

```
diagnose dvm task list <adom> <type>
diagnose dvm task repair
diagnose dvm task reset
```

Variable	Description
list <adom> <type>	List task database information.
repair	Repair the task database while preserving existing data where possible. The FortiAnalyzer will reboot after the repairs.
reset	Reset the task database to its factory default state. All existing tasks and the task history will be erased. The FortiAnalyzer will reboot after the reset.

dvm taskline

Use this command to repair the task lines.

Syntax

```
diagnose dvm taskline repair
```

Variable	Description
repair	Repair the task lines while preserving data wherever possible. The FortiAnalyzer will reboot after the repairs.

dvm transaction-flag

Use this command to edit or display DVM transaction flags.

Syntax

```
diagnose dvm transaction-flag [abort | debug | none]
```

Variable	Description
transaction-flag [abort debug none]	Set the transaction flag.

dvm workflow

This command does not function on FortiAnalyzer.

faz-cdb

Use these commands for FortiAnalyzer database configuration related settings.

faz-cdb fix

Use this command to fix the FortiAnalyzer configuration database.

Syntax

```
diagnose faz-cdb fix check-report-folder <adom name>
diagnose faz-cdb fix fix-report-folder <adom name>
```

Variable	Description
check-report-folder	Check FortiAnalyzer configuration database report folders from the last upgrade backup.
fix-report-folder	Fix FortiAnalyzer configuration database report folders from the last upgrade.
<adom name>	Enter the ADOM name or enter <code>all</code> for all ADOMs.

faz-cdb reset

Use this command to reset the FortiAnalyzer configuration database.

Syntax

```
diagnose faz-cdb reset
```

faz-cdb upgrade

Use this command to upgrade the FortiAnalyzer configuration database.

Syntax

```
diagnose faz-cdb upgrade check-adom <adom name>
diagnose faz-cdb upgrade check-global
diagnose faz-cdb upgrade export-config <adom name> <service> <ip> <user> <password>
    <path/filename>
diagnose faz-cdb upgrade import-config <adom name> <service> <ip> <user> <password>
    <path/filename>
diagnose faz-cdb upgrade log
diagnose faz-cdb upgrade summary
```

Variable	Description
check-adom	Check the last ADOM upgrade result.
check-global	Check the last global upgrade result.
export-config	Export the FortiAnalyzer configuration database files.
import-config	Import the FortiAnalyzer configuration database files.
log	Display the FortiAnalyzer configuration database upgrade log.
summary	Display the FortiAnalyzer configuration database summary.
<adom name>	Enter the ADOM name or enter <code>all</code> for all ADOMs.
<service>	Enter the transfer protocol one of: <code>ftp</code> , <code>sftp</code> , or <code>scp</code> .
<ip>	Enter the server IP address. For FTP, the port can be specified by adding <code>:port</code> to the server IP address.
<user>	Enter a user name of the remote server.
<password>	Enter the password or <code>' '</code> for user.
<path/filename>	Enter the path/ filename on remote server.

fmnetwork

Use the following commands for network related settings.

fmnetwork arp

Use this command to manage ARP.

Syntax

```
diagnose fmnetwork arp del <intf-name> <ip>
diagnose fmnetwork arp list
```

Variable	Description
del <intf-name> <ip>	Delete an ARP entry.
list	List ARP entries.

fmnetwork interface

Use this command to view interface information.

Syntax

```
diagnose fmnetwork interface detail <interface>
diagnose fmnetwork interface list [<interface>]
```

Variable	Description
detail <interface>	View a specific interface's details, for example: port1.
list [<interface>]	List all interface details.

fmnetwork netstat

Use this command to view network statistics.

Syntax

```
diagnose fmnetwork netstat list [-r]
diagnose fmnetwork netstat tcp [-r]
diagnose fmnetwork netstat udp [-r]
```

Variable	Description
list [-r]	List all connections, or use -r to list only resolved IP addresses.
tcp [-r]	List all TCP connections, or use -r to list only resolved IP addresses.
udp [-r]	List all UDP connections, or use -r to list only resolved IP addresses.

fmupdate

Use these commands to diagnose update services.

Syntax

```

diagnose fmupdate check-disk-quota {export-import | fds | fgd | all} <clean>
diagnose fmupdate crdb {generate | view}
diagnose fmupdate dbcontract [<serial>]
diagnose fmupdate del-device <serial>
diagnose fmupdate del-log
diagnose fmupdate del-object {fds | fgd | fqfq | geoip} [<object_type>] [<object_
    version>]
diagnose fmupdate del-serverlist {fct | fds | fgd}
diagnose fmupdate dump-um-db {um2.db | fds.db} [<table>]
diagnose fmupdate fds-dump {breg | fds-log | fect | fmgi | imlt | imlt-d | immx | oblt |
    srul | subs}
diagnose fmupdate fds-getobject <filter type> <filter> <other options>
diagnose fmupdate fds-update-info
diagnose fmupdate fgd-bandwidth {1h | 6h | 12h | 24h | 7d | 30d}
diagnose fmupdate fgd-dbver [{as1 | as2 | as4 | av | av2 | cat1 | fq | geoip | iotm |
    iotr | iots | wf}]
diagnose fmupdate fgd-del-db [{as1 | as2 | as4 | av | av2 | cat1 | fq | geoip | iotm |
    iotr | iots | wf}]
diagnose fmupdate fgd-dump [{as1 | as2 | as4 | av | av2 | cat1 | fq | geoip | iotm | iotr
    | iots | wf}]
diagnose fmupdate fgd-test-client <ip> <serial> <string> <integer>
diagnose fmupdate fgd-url-rating <ip> <serial> <version> <url>
diagnose fmupdate fgd-wfas-clear-log
diagnose fmupdate fgd-wfas-log [{name | ip} {<name> | <ip addr>}]
diagnose fmupdate fgd-wfas-rate [{as_hash | as_ip | as_url | av | av2 | fq | wf}]
diagnose fmupdate fgd-wfdevice-stat {10m | 30m | 1h | 6h | 12h | 24h | 7d} <serial>
    <integer>
diagnose fmupdate fgd-wfserver-stat {top10sites | top10devices} [{10m | 30m | 1h | 6h |
    12h | 24h | 7d}]
diagnose fmupdate fgt-del-statistics
diagnose fmupdate fgt-del-um-db [{um.db | um2.db | fds.db | um_stat.db}]
diagnose fmupdate fmg-statistic-info
diagnose fmupdate fortitoken {seriallist | add | del} <serial>
diagnose fmupdate list-object {fds | fgd | fgfq | geoip} [<object_type>] [<object_
    version>]
diagnose fmupdate priority-download {clear | list | view}
diagnose fmupdate service-restart {fds | fgd | fmtr | fwm}
diagnose fmupdate show-bandwidth {fct | fgt | fml | faz} {1h | 6h | 12h | 24h | 7d | 30d}
diagnose fmupdate show-dev-obj [<serial>]

```



```

diagnose fmupdate update-status {fds | fct | fgd}
diagnose fmupdate updatenow {fds | fgd} {fgd | fgfq | geoip} {SelectivePoll | Poll | Consolidation | Command}
diagnose fmupdate view-configure {fds | fct | fgd | fmtr}
diagnose fmupdate view-linkd-log {fct | fds | fgd}
diagnose fmupdate view-serverlist {fds | fgd}
diagnose fmupdate view-service-info {fds | fgd}
diagnose fmupdate vm-license

```

Variables	Description
check-disk-quota {export-import fds fgd all} <clean>	Check the related directory size. Clean the export/import directory, if necessary.
crdb {generate view}	Generate or view certificate files from the database.
dbcontract [<serial>]	Dump the subscriber contract.
del-device <serial>	Delete a device.
del-log	Delete all the logs for FDS and FortiGuard update events.
del-object {fds fgd fgfq geoip} [<object_type>] [<object_version>]	Remove all objects from the specified service. Optionally, enter the object type and version or time.
del-serverlist {fct fds fgd}	Delete the server list file (fdni.dat) from the specified service.
dump-um-db {um2.db fds.db} [<table>]	Dump um databases or dump either um2 or fds database. Optionally, you can dump a specified table in um2 or fds databases.
fds-dump {breg fds-log fect fmgi imlt imlt-d immx oblt srul subs}	Dump FDS files: <ul style="list-style-type: none"> • breg: Dump the FDS beta serial numbers. • fds-log: Dump the FDS svrd log. Optionally, enter a rolling number from 0 to 10. • fect: Dump the FortiClient image file. Choose from the two available options of dumping the FortiClient file for the server or the client. • fmgi: Dump FMGI (Object description details) file. • imlt: Dump FGT image list file. • imlt-d: Dump FGT image file for downstream device. • immx: Dump the image upgrade matrix file. You can dump the IMMX files for FortiManager, FortiGate, or FortiCloud. • oblt: Dump the object list file. You can dump the object list files for FortiGate or FortiClient service. • srul: Dump the FDS select filtering rules. • subs: Dump Contract file.
fds-getobject <filter type> <filter> <other options>	Get the versions of all FortiGate objects for antivirus-IPS. <ul style="list-style-type: none"> • <filter type>: Enter <code>product</code> or <code>objid</code> as the filter type. • <filter>: Enter an available filters. These filters are available only when you select <code>product</code> as your filter type. Enter <code>all</code> for all product filters. • <other options>: Enter <code>used</code> to show used-only objects or <code>raw</code> to show response in raw JSON format.

Variables	Description
fds-update-info	Display scheduled update information.
fgd-bandwidth {1h 6h 12h 24h 7d 30d}	Display the download bandwidth.
fgd-dbver [{as1 as2 as4 av av2 cat1 fq geoip iotm iotr iots wf}]	Get the version of the database. Optionally, enter the database type: <ul style="list-style-type: none"> as1: Antispam (IP). as2: Antispam (URL). as4: Antispam (HASH). av: AntiVirus Query. av2: Outbreak Prevention. cat1: Query Category. fq: File Query. geoip: GeoIP. iotm: IoT (mapping). iotr: IoT (range). iots: IoT (single). wf: Webfilter.
fgd-del-db [{as1 as2 as4 av av2 cat1 fq geoip iotm iotr iots wf}]	Delete FortiGuard database. Optionally, enter the database type: <ul style="list-style-type: none"> as1: Antispam (IP). as2: Antispam (URL). as4: Antispam (HASH). av: AntiVirus Query. av2: Outbreak Prevention. cat1: Query Category. fq: File Query. geoip: GeoIP. iotm: IoT (mapping). iotr: IoT (range). iots: IoT (single). wf: Webfilter.
fgd-dump [{as1 as2 as4 av av2 cat1 fq geoip iotm iotr iots wf}]	Dump the FortiGuard information. Optionally, enter the database type: <ul style="list-style-type: none"> as1: Antispam (IP). as2: Antispam (URL). as4: Antispam (HASH). av: AntiVirus Query. av2: Outbreak Prevention. cat1: Query Category. fq: File Query. geoip: GeoIP. iotm: IoT (mapping).

Variables	Description
	<ul style="list-style-type: none"> • <code>iotr</code>: IoT (range). • <code>iots</code>: IoT (single). • <code>wf</code>: Webfilter.
<code>fgd-test-client <ip> <serial> <string> <integer></code>	<p>Execute FortiGuard test client.</p> <ul style="list-style-type: none"> • <code><ip></code>: Enter the hostname or IP of the FortiGuard server. • <code><serial></code>: Enter the serial number of the device. • <code><string></code>: Enter the query number per second for stress test, or enter URL for a single query. • <code><integer></code>: Optionally, enter the category version (default = 7).
<code>fgd-url-rating <ip> <serial> <version> <url></code>	<p>Rate URLs within the FortiManager database using the FortiGate serial number. Optionally, enter the category version and URL.</p>
<code>fgd-wfas-clear-log</code>	<p>Clear the FortiGuard service log file.</p>
<code>fgd-wfas-log [{name ip} {<name> <ip addr>}]</code>	<p>View the FortiGuard service log file. Optionally, enter the device filter type, and device name or IPv4 address.</p>
<code>fgd-wfas-rate [{as_hash as_ip as_url av av2 fq wf}]</code>	<p>Get the web filter / antispam rating speed. Optionally, enter the server type:</p> <ul style="list-style-type: none"> • <code>as_hash</code>: Antispam (HASH). • <code>as_ip</code>: Antispam (IP). • <code>as_url</code>: Antispam (URL). • <code>av</code>: AntiVirus Query. • <code>av2</code>: Outbreak Prevention. • <code>fq</code>: File Query. • <code>wf</code>: Webfilter.
<code>fgd-wfdevice-stat {10m 30m 1h 6h 12h 24h 7d} <serial> <integer></code>	<p>Display web filter device statistics. Enter <code>all</code> or a specific device's serial number. Optionally, enter the number of time periods to display (default = 1).</p>
<code>fgd-wfserver-stat {top10sites top10devices} [{10m 30m 1h 6h 12h 24h 7d}]</code>	<p>Display web filter server statistics for the top 10 sites or devices. Optionally, enter the time frame to cover.</p>
<code>fgt-del-statistics</code>	<p>Remove all statistics (antivirus / IPS and web filter / antispam). This command requires a reboot.</p>
<code>fgt-del-um-db [{um.db um2.db fds.db um_stat.db}]</code>	<p>Remove <code>UM</code>, <code>UM2</code>, <code>fds</code>, and <code>um_stat</code> databases. This command requires a reboot.</p> <p>Note: <code>um.db</code> is a sqlite3 database that update manager uses internally. It will store AV/IPS package information of downloaded packages. This command removes the database file information. The package is not removed. After the reboot, the database will be recreated. Use this command if you suspect the database file is corrupted.</p>
<code>fmg-statistic-info</code>	<p>Display statistic information for FortiManager and Java Client.</p>

Variables	Description
fortitoken {seriallist add del} <serial>	FortiToken related operations.
list-object {fds fgd fgfq geoip} [<object_type>] [<object_version>]	List downloaded objects of linkd service. Optionally, enter the object type and version or time.
priority-download {clear list view}	Command for priority download: <ul style="list-style-type: none"> clear: view config. list: list object id of list. view: clear config.
service-restart {fds fgd fmtr fwm}	Restart the linkd service.
show-bandwidth {fct fgt fml faz} {1h 6h 12h 24h 7d 30d}	Display the download bandwidth for a device type over a specified time period.
show-dev-obj [<serial>]	Display an objects version of a device. Optionally, enter a serial number.
update-status {fds fct fgd}	Display the update status.
updatenow {fds fgd} {fgd fgfq geoip} {SelectivePoll Poll Consolidation Command}	Update immediately. Select a service, service type, and task type. Note: Selecting a service and task type is only available when the service is fgd.
view-configure {fds fct fgd fmtr}	Dump the running configuration.
view-linkd-log {fct fds fgd}	View the linkd log file.
view-serverlist {fds fgd}	Dump the server list.
view-service-info {fds fgd}	Display the service information.
vm-license	Dump the FortiGate VM license.

fortilogd

Use this command to view FortiLog daemon information.

Syntax

```
diagnose fortilogd lograte
diagnose fortilogd lograte-adom
diagnose fortilogd lograte-device [filter]
diagnose fortilogd lograte-total
diagnose fortilogd lograte-type
diagnose fortilogd logvol-adom
diagnose fortilogd msgrate
diagnose fortilogd msgstat [flush]
```

```
diagnose fortilogd status
```

Variable	Description
lograte	Display the log rate.
lograte-adom	Display log rate by ADOM.
lograte-device [filter]	Display log rate by device.
lograte-total	Display log rate by total.
lograte-type	Display log rate by type.
logvol-adom	Display the GB/day by ADOM.
msgrate	Display log message rate.
msgstat [flush]	Display or flush log message statuses.
status	Running status.

fortirecorder

Use the following commands to diagnose fortirecorder related settings.

It is only available on hardware devices that support FortiRecorder.

Syntax

```
diagnose fortirecorder camera stats recordings [camera name]
diagnose fortirecorder ftp-password
```

Variable	Description
camera stats recordings [camera name]	View the camera recording statistics (number of files, total, size, and total duration) for all cameras, or a specific camera.
ftp-password	View the FTP password for camera uploading.

fwmanager

Use these commands to manage firmware.

Syntax

```
diagnose fwmanager fwm-log <dump> [rolling number]
diagnose fwmanager image-clear
diagnose fwmanager image-delete <file>
diagnose fwmanager image-download <platform> <version>
```

```

diagnose fwmanager image-list <product>
diagnose fwmanager profile {list | sync | clear} [adom]
diagnose fwmanager service-restart
diagnose fwmanager set-controller-schedule <device> <controller_id> <version> [date_time]
diagnose fwmanager set-dev-schedule <device> <version> [flags] [date_time]
diagnose fwmanager set-grp-schedule <group> <version> [flags] [date_time]
diagnose fwmanager show-dev-disk-check-status <device>
diagnose fwmanager show-dev-upgrade-path <device> <version>
diagnose fwmanager show-grp-disk-check-status <group>
diagnose fwmanager test-upgrade-path <platform> <from-version> <to-version> [debug]

```

Variable	Description
fwm-log <dump> [rolling number]	View the firmware manager log file. Optionally, dump whole log. Optionally, enter a rolling number from 0 to 10.
image-clear	Clear all local images and its FCP object files.
image-delete <file>	Delete a local image.
image-download <platform> <version>	Download the official image. Enter the platform name and version.
image-list <product>	Get the local firmware image list for the product: <ul style="list-style-type: none"> • FGT: FortiGate • FMG: FortiManager • FAZ: FortiAnalyzer • FAP: FortiAP • FSW: FortiSwitch • FXT: FortiExtender
profile {list sync clear} [adom]	List, synchronize with the database, or clear the firmware profile setting. Optionally, enter the adom name.
service-restart	Restart the firmware manager server.
set-controller-schedule <device> <controller_id> <version> [date_ time]	Create a controller upgrade schedule for a device.
set-dev-schedule <device> <version> [flags] [date_time]	Create an upgrade schedule for a device.
set-grp-schedule <group> <version> <flags> <date_time>	Create an upgrade schedule for a group.
show-dev-disk-check-status <device>	Show whether the device needs a disk check.
show-dev-upgrade-path <device> <version>	Show the possible upgrade path.
show-grp-disk-check-status <group>	Show whether the devices in the group need disk checks.

Variable	Description
test-upgrade-path <platform> <from-version> <to-version> [debug]	Show possible FortiGate upgrade paths.

ha

Use this command to view and manage high availability.

Syntax

```
diagnose ha check-data {start | stop | status}
diagnose ha data-check-report {read | delete}
diagnose ha dump-datalog
diagnose ha failover <device-id>
diagnose ha force-cfg-resync
diagnose ha load-balance
diagnose ha logs
diagnose ha restart-init-sync
diagnose ha request-init-sync
diagnose ha stats [verbose]
diagnose ha status
diagnose ha trace-client-req {enable | disable}
```

Variable	Description
check-data {start stop status}	Start/stop or check status of database hash and revision files.
data-check-report {read delete}	Read or delete the data check validation report.
dump-datalog	Dump the HA data log.
failover <device-id>	Force HA failover. Use the device ID of the new primary device, or re-elect from backup FortiAnalyzer devices if not specified.
force-cfg-resync	Force HA to re-synchronize the configuration.
load-balance	HA load balance status.
logs	Get HA logs.
restart-init-sync	Restart HA initial sync. This command can only be run on the primary unit.
request-init-sync	Request to redo HA initial sync. This command can only be run on the secondary unit.
stats [verbose]	Get HA statistics. Optionally, get verbose output.
status	Get HA status.
trace-client-req {enable disable}	Enable/disable trace of client side request.

hardware

Use this command to view hardware information. This command provides comprehensive system information including: CPU, memory, disk, and RAID information.

Syntax

```
diagnose hardware info
```

incident

Use this command to view incident attachment information

Syntax

```
diagnose incident attachment status <adom> <attachment type> [detail]
```

Variable	Description
attachment	Incident's Attachment.
status	Attachment status information.
<adom>	ADOM name or <code>all</code> for all ADOMs.
<attachment type>	The attachment type: <code>report</code> , <code>alertevent</code> , <code>note</code> , <code>file</code> , or <code>all</code> for all types.
[detail]	Show detailed information.

license

Use this command to check license information.

Syntax

```
diagnose license list
diagnose license update
```

Variable	Description
list	List the FortiAnalyzer license information.
update	Update the FortiAnalyzer license information.

log

Use the following command to view device log usage and log rate limiting information.

Syntax

```
diagnose log device [<device-id> | adom] [adom-name | all | *]  
diagnose log ratelimit
```

Variable	Description
[<device-id> adom]	Optionally filter by device ID or ADOM.
[adom-name all *]	Optional filter by ADOM name when filtering by ADOM.

pm2

Use these commands to check the integrity of the database.

Syntax

```
diagnose pm2 check-integrity {all adom device global ips task ncldb}  
diagnose pm2 print <log-type>
```

Variable	Description
check-integrity {all adom device global ips task ncldb}	Check the integrity of the database. Multiple database categories can be selected.
print <log-type>	Print the database log messages.

report

Use this command to check the SQL database.

Syntax

```
diagnose report clean {ldap-cache | report-queue}  
diagnose report status [pending | running]
```

Variable	Description
clean {ldap-cache report-queue}	Cleanup the SQL report queue or LDAP cache.
status [pending running]	Check status information on pending and running reports.

rtm

Use this command to display or update real time monitor profile database.

Syntax

```
diagnose rtm profile
```

siem

Use this command to check the SIEM database.

Syntax

```
diagnose siem process list full
diagnose siem process kill <query_id>
diagnose siem module-ctrl {enable | disable}
diagnose siem remove database <adom>
diagnose siem service {start | stop}
```

Variable	Description
process list full	List the query processes and its details.
process kill <query_id>	Kill a running query. Enter the query ID.
module-ctrl {enable disable}	Enable/disable the SIEM module. This command is only available on hardware based devices.
remove database <adom>	Remove the SIEM database from the specified ADOM, or all ADOMs.
service {start stop}	Start/stop the SIEM service. This command is only available on VM based devices.

sniffer

Use this command to perform a packet trace on one or more network interfaces.

Packet capture, also known as sniffing, records some or all of the packets seen by a network interface. By recording packets, you can trace connection states to the exact point at which they fail, which may help you to diagnose some types of problems that are otherwise difficult to detect.

FortiAnalyzer units have a built-in sniffer. Packet capture on FortiAnalyzer units is similar to that of FortiGate units. Packet capture is displayed on the CLI, which you may be able to save to a file for later analysis, depending on your CLI client.

Packet capture output is printed to your CLI display until you stop it by pressing **CTRL + C**, or until it reaches the number of packets that you have specified to capture.



Packet capture can be very resource intensive. To minimize the performance impact on your FortiAnalyzer unit, use packet capture only during periods of minimal traffic, with a serial console CLI connection rather than a Telnet or SSH CLI connection, and be sure to stop the command when you are finished.

Syntax

```
diagnose sniffer packet <interface> <filter> <verbose> <count> <Timestamp format>
```

Variable	Description
<interface>	Type the name of a network interface whose packets you want to capture, such as <code>port1</code> , or type <code>any</code> to capture packets on all network interfaces.
<filter>	<p>Type either <code>none</code> to capture all packets, or type a filter that specifies which protocols and port numbers that you do or do not want to capture, such as <code>'tcp port 25'</code>. Surround the filter string in quotes.</p> <p>The filter uses the following syntax:</p> <pre>'[[src dst] host {<host1_fqdn> <host1_ipv4>}] [and or] [[src dst] host {<host2_fqdn> <host2_ipv4>}] [and or] [[arp ip gre esp udp tcp] port <port1_int>] [and or] [[arp ip gre esp udp tcp] port <port2_int>]'</pre> <p>To display only the traffic between two hosts, specify the IP addresses of both hosts. To display only forward or only reply packets, indicate which host is the source and which is the destination.</p> <p>For example, to display UDP port 1812 traffic between 1.example.com and either 2.example.com or 3.example.com, you would enter:</p> <pre>'udp and port 1812 and src host 1.example.com and dst \ (2.example.com or 2.example.com \)'</pre>
<verbose>	<p>Type one of the following numbers indicating the depth of packet headers and payloads to capture:</p> <ul style="list-style-type: none"> 1: print header of packets (default) 2: print header and data from ip of packets 3: print header and data from ethernet of packets (if available) <p>For troubleshooting purposes, Fortinet Technical Support may request the most verbose level (3).</p>
<count>	<p>Type the number of packets to capture before stopping.</p> <p>If you do not specify a number, the command will continue to capture packets until you press CTRL + C.</p>
<Timestamp format>	<p>Type the timestamp format.</p> <ul style="list-style-type: none"> a: absolute UTC time, yyyy-mm-dd hh:mm:ss.ms l: absolute LOCAL time, yyyy-mm-dd hh:mm:ss.ms otherwise: relative to the start of sniffing, ss.ms

Example 1

The following example captures the first three packets' worth of traffic, of any port number or protocol and between any source and destination (a filter of `none`), that passes through the network interface named `port1`. The capture uses a low level of verbosity (indicated by `1`).

Commands that you would type are highlighted in bold; responses from the Fortinet unit are not in bold.

```
FortiAnalyzer# diag sniffer packet port1 none 1 3
interfaces=[port1]
filters=[none]
0.918957 192.168.0.1.36701 -> 192.168.0.2.22: ack 2598697710
0.919024 192.168.0.2.22 -> 192.168.0.1.36701: psh 2598697710 ack 2587945850
0.919061 192.168.0.2.22 -> 192.168.0.1.36701: psh 2598697826 ack 2587945850
```

If you are familiar with the TCP protocol, you may notice that the packets are from the middle of a TCP connection. Because port 22 is used (highlighted above in bold), which is the standard port number for SSH, the packets might be from an SSH session.

Example 2

The following example captures packets traffic on TCP port 80 (typically HTTP) between two hosts, 192.168.0.1 and 192.168.0.2. The capture uses a low level of verbosity (indicated by `1`). Because the filter does not specify either host as the source or destination in the IP header (`src` or `dst`), the sniffer captures both forward and reply traffic.

A specific number of packets to capture is not specified. As a result, the packet capture continues until the administrator presses CTRL + C. The sniffer then confirms that five packets were seen by that network interface.

Commands that you would type are highlighted in bold; responses from the Fortinet unit are not in bold.

```
FortiAnalyzer# diag sniffer packet port1 'host 192.168.0.2 or host 192.168.0.1 and tcp
port 80' 1
192.168.0.2.3625 -> 192.168.0.1.80: syn 2057246590
192.168.0.1.80 -> 192.168.0.2.3625: syn 3291168205 ack 2057246591
192.168.0.2.3625 -> 192.168.0.1.80: ack 3291168206
192.168.0.2.3625 -> 192.168.0.1.80: psh 2057246591 ack 3291168206
192.168.0.1.80 -> 192.168.0.2.3625: ack 2057247265
5 packets received by filter
0 packets dropped by kernel
```

Example 3

The following example captures all TCP port 443 (typically HTTPS) traffic occurring through `port1`, regardless of its source or destination IP address. The capture uses a high level of verbosity (indicated by `3`).

A specific number of packets to capture is not specified. As a result, the packet capture continues until the administrator presses CTRL + C. The sniffer then confirms that five packets were seen by that network interface.

Verbose output can be very long. As a result, output shown below is truncated after only one packet.

Commands that you would type are highlighted in bold; responses from the Fortinet unit are not in bold.

```
FortiAnalyzer # diag sniffer port1 'tcp port 443' 3
interfaces=[port1]
filters=[tcp port 443]
10.651905 192.168.0.1.50242 -> 192.168.0.2.443: syn 761714898
0x0000 0009 0f09 0001 0009 0f89 2914 0800 4500 .....E.
```

```

0x0010 003c 73d1 4000 4006 3bc6 d157 fede ac16 .<s.@.@.;..W....
0x0020 0ed8 c442 01bb 2d66 d8d2 0000 0000 a002 ...B..-f.....
0x0030 16d0 4f72 0000 0204 05b4 0402 080a 03ab ..Or.....
0x0040 86bb 0000 0000 0103 0303 .....

```

Instead of reading packet capture output directly in your CLI display, you usually should save the output to a plain text file using your CLI client. Saving the output provides several advantages. Packets can arrive more rapidly than you may be able to read them in the buffer of your CLI display, and many protocols transfer data using encodings other than US-ASCII. It is usually preferable to analyze the output by loading it into a network protocol analyzer application such as Wireshark (<http://www.wireshark.org/>).

For example, you could use PuTTY or Microsoft HyperTerminal to save the sniffer output. Methods may vary. See the documentation for your CLI client.

Requirements

- terminal emulation software such as [PuTTY](#)
- a plain text editor such as Notepad
- a [Perl](#) interpreter
- network protocol analyzer software such as [Wireshark](#)

To view packet capture output using PuTTY and Wireshark:

1. On your management computer, start PuTTY.
2. Use PuTTY to connect to the Fortinet appliance using either a local serial console, SSH, or Telnet connection.
3. Type the packet capture command, such as:

```
diagnose sniffer packet port1 'tcp port 541' 3 100
```

but do not press `Enter` yet.
4. In the upper left corner of the window, click the PuTTY icon to open its drop-down menu, then select *Change Settings*.
A dialog appears where you can configure PuTTY to save output to a plain text file.
5. In the *Category* tree on the left, go to *Session > Logging*.
6. In *Session logging*, select *Printable output*.
7. In *Log file name*, click the *Browse* button, then choose a directory path and file name such as `C:\Users\MyAccount\packet_capture.txt` to save the packet capture to a plain text file. (You do not need to save it with the `.log` file extension.)
8. Click *Apply*.
9. Press `Enter` to send the CLI command to the FortiMail unit, beginning packet capture.
10. If you have not specified a number of packets to capture, when you have captured all packets that you want to analyze, press `CTRL + C` to stop the capture.
11. Close the PuTTY window.
12. Open the packet capture file using a plain text editor such as Notepad++.
13. Delete the first and last lines, which look something like this:

```

===== PuTTY log 2023.09.29 08:03:40 =====
Fortinet-2000 #

```

These lines are a PuTTY timestamp and a command prompt, which are not part of the packet capture. If you do not delete them, they could interfere with the script in the next step.
14. Convert the plain text file to a format recognizable by your network protocol analyzer application.
You can convert the plain text file to a format (`.pcap`) recognizable by Wireshark using the `fgt2eth.pl` Perl script. To download `fgt2eth.pl`, see the [Fortinet Knowledge Base](#) article [Using the FortiOS built-in packet sniffer](#).



The fgt2eth.pl script is provided as-is, without any implied warranty or technical support, and requires that you first install a Perl module compatible with your operating system.

To use fgt2eth.pl, open a command prompt, then enter a command such as the following:

```
fgt2eth.pl -in packet_capture.txt -out packet_capture.pcap
```

where:

- `fgt2eth.pl` is the name of the conversion script; include the path relative to the current directory, which is indicated by the command prompt
- `packet_capture.txt` is the name of the packet capture's output file; include the directory path relative to your current directory
- `packet_capture.pcap` is the name of the conversion script's output file; include the directory path relative to your current directory where you want the converted output to be saved

15. Open the converted file in your network protocol analyzer application. For further instructions, see the documentation for that application.

For additional information on packet capture, see the Fortinet Knowledge Base article [Using the FortiOS built-in packet sniffer](#).

sql

Use this command to diagnose the SQL database.

sql config

Use this command to show, set, or reset the SQL database configuration.

Syntax

```
diagnose sql config auto-cache-delay [set <seconds>| reset]
diagnose sql config debug-filter [set | test] <daemon> <string>
diagnose sql config deferred-index-timespan [set <value>]
diagnose sql config hcache-agg-step [reset | set <integer>]
diagnose sql config hcache-base-trim-interval [reset | set <integer>]
diagnose sql config hcache-max-base-row [reset | set <integer>]
diagnose sql config hcache-max-fv-row [reset | set <integer>]
diagnose sql config hcache-max-fv-row-per-timescale [reset | set <integer>]
diagnose sql config hcache-max-rpt-row [reset | set <integer>]
diagnose sql config sampling-max-row [reset | set <integer>]
diagnose sql config sampling-status [reset | set <integer>]
diagnose sql config sampling-type [reset | set <integer>]
```

Variable	Description
auto-cache-delay [set <seconds> reset]	Show, set, or reset the auto-cache delay, in seconds (default = 300).

Variable	Description
debug-filter {set test} <daemon> <string>	Show sqlplugind and sqlreportd debug filter. Enter sqlplugind, sqlreportd or both as the <daemon>. Enter the filter string.
deferred-index-timespan [set <value>]	View or set the time span for the deferred index (default = 10000).
hcache-agg-step [reset set <integer>]	Show, set, or reset the hcache aggregation step (default = 10).
hcache-base-trim-interval [reset set <integer>]	Show, set, or reset the hcache base trim interval (3600 - 2147483647, default = 172800).
hcache-max-base-row [reset set <integer>]	Show, set, or reset max row number for base hcache (1000 - 1500000, default = 1000000).
hcache-max-fv-row [reset set <integer>]	Show, set, or reset max row number for fortiview hcache (1000 - 400000, default = 50000).
hcache-max-fv-row-per-timescale [reset set <integer>]	Show, set, or reset max row number per timescale for FortiView hcache (0 - 40000, default = 0).
hcache-max-rpt-row [reset set <integer>]	Show, set, or reset max row number for report hcache (1000 - 400000, default = 18000).
sampling-max-row [reset set <integer>]	Show, set, or reset max row number for sampling (1000 - 10000000, default = 1000000).
sampling-status [reset set <integer>]	Show, set, or reset the sampling status. Enter 0 for disabling and 1 for enabling the sample status (0 - 1, default = 1).
sampling-type [reset set <integer>]	Show, set, or reset the type of sampling (0 - 1, default = 0).

sql debug

Use this command to show or update the SQL debug statuses.

Syntax

```

diagnose sql debug hcache-agg dbgoff
diagnose sql debug hcache-agg dbgon
diagnose sql debug hcache-agg delete
diagnose sql debug hcache-agg show [<filter>] [<NUM>]
diagnose sql debug hcache-agg upload {ftp | sftp} <host> <dir> <user name> <password>
diagnose sql debug logview dbgoff
diagnose sql debug logview dbgon <level value>
diagnose sql debug logview delete
diagnose sql debug logview show [<filter>] [<NUM>]
diagnose sql debug logview upload {ftp | sftp} <host> <dir> <user name> <password>
diagnose sql debug pglog show [<filter>] [<NUM>]
diagnose sql debug pglog upload {ftp | sftp} <host> <dir> <user name> <password>
diagnose sql debug sqlqry dbgoff
diagnose sql debug sqlqry dbgon <level value>

```

```

diagnose sql debug sqlqry delete
diagnose sql debug sqlqry show [<filter>][<NUM>]
diagnose sql debug sqlqry upload {ftp | sftp} <host> <dir> <user name> <password>

```

Variable	Description
hcache-agg dbgoff	Disable hcache-agg debug output.
hcache-agg dbgon	Enable hcache-agg debug output.
hcache-agg delete	Delete hcache-agg debug file.
hcache-agg show [<filter>] [<NUM>]	Show the last 10 lines of the hcache-agg debug file. Set filter for the debug file, and show the last NUM lines of the debug file. The filter and NUM variables are optional.
hcache-agg upload {ftp sftp} <host> <dir> <user name> <password>	Upload hcache-agg debug file to FTP or SFTP server. Enter host IP address, directory, user name, and password.
logview dbgoff	Disable Log view debug output.
logview dbgon <level value>	Enable log view debug output. Set log view debug level (1-5). Default level is 1.
logview delete	Delete log view debug file.
logview show [<filter>] [<NUM>]	Show the last 10 lines of the Log view debug file. Set filter for debug file, and show last NUM lines of the debug file. The filter and NUM variables are optional.
logview upload {ftp sftp} <host> <dir> <user name> <password>	Upload log view debug file to FTP or SFTP server. Enter host IP address, directory, user name, and password.
pglog show [<filter>] [<NUM>]	Show the last 10 lines of the Postgres log debug file. Set filter for debug file, and show last NUM lines of the debug file. The filter and NUM variables are optional.
pglog upload {ftp sftp} <host> <dir> <user name> <password>	Upload Postgres log debug file to FTP or SFTP server. Enter host IP address, directory, user name, and password.
sqlqry dbgoff	Disable SQL query debug output.
sqlqry dbgon <level value>	Enable SQL query debug output. Set SQL query debug level (1-5). The default level is 1. Note: When the debug level is 5, the final SQL running in sqlreportd will show in the debug output as well.
sqlqry delete	Delete the SQL query debug file.
sqlqry show [<filter>] [<NUM>]	Show the last 10 lines of the SQL query debug file. Set filter for the debug file, and show the last NUM lines of the debug file. The filter and NUM variables are optional.
sqlqry upload {ftp sftp} <host> <dir> <user name> <password>	Upload SQL query debug file to FTP or SFTP server. Enter host IP address, directory, user name, and password.

sql hcache

Use this command to show or update the SQL hcache.

Syntax

```

diagnose sql hcache add-task agg <adom> <norm-query-hash> <agg-level> <timestamp> <num-
of-days>
diagnose sql hcache add-task agg-update <adom> <hid>
diagnose sql hcache dump-task <filter>
diagnose sql hcache list <adom> <query-hash/tag> <filter> <detail>
diagnose sql hcache plan <adom> <start-time> <end-time> <query-tag/norm-qry-hash/sql>
<is-fortiview> <max-time-scale>
diagnose sql hcache rebuild-both <start-time> <end-time>
diagnose sql hcache rebuild-fortiview <start-time> <end-time>
diagnose sql hcache rebuild-report <start-time> <end-time>
diagnose sql hcache rebuild-status
diagnose sql hcache show hcache <adom> <id>
diagnose sql hcache show hcache-query <adom> <norm-qry-hash>
diagnose sql hcache show hcache-res-tbl <adom> <res-tbl-id>
diagnose sql hcache show time <time> <time> <time> <time>
diagnose sql hcache status {all | <adom> | all-summary}

```

Variable	Description
add-task agg <adom> <norm-query-hash> <agg-level> <timestamp> <num-of-days>	<p>Add an hcache agg task. The following input is required:</p> <ul style="list-style-type: none"> adom: The ADOM name. norm-query-hash: The normalized query hash. agg-level: The aggregation level. timestamp: The timestamp (format = yyyy-mm-dd hh:mm:ss). num-of-days: The number of days (1, 3, or 30).
add-task agg-update <adom> <hid>	<p>Add an hcache agg update task. The following input is required:</p> <ul style="list-style-type: none"> adom: The ADOM name. hid: The hcache agg ID.
dump-task <filter>	<p>Dump hcache tasks. Enter the task filter.</p>
list <adom> <queryhash/tag> <filter> <detail>	<p>List hcache:</p> <ul style="list-style-type: none"> adom: The ADOM name. query-hash/tag: The hash or tag filter query, or all for all queries. filter: Narrow down the hcache list search result by using a filter. The filter keywords include: <ul style="list-style-type: none"> status: The hcache status. 0(Ready), 1(Ready-Loss), 2(In-Building), 3(Error), 4(Invalid-SQL), 5(No-Data), 6(Not-Ready). fv_flag: List FortiView/report only. 1(fortiview), 0(report). sql: The SQL query match. '*' for wildcard, e.g. *select*. time_start: Start of the log time. format: yyyy-mm-dd hh:MM:ss. time_end: End of the log time. format: yyyy-mm-dd hh:MM:ss. <p>The following shows an example of the variable <filter>:</p> <pre>"status=0,1,5 sql=\"*srcip, dstip*\" time_start>=\"2020-11-01 00:00:00\" time_end<=\"2020-11-30 23:59:59\""</pre> <p>Enter "" for no filter.</p> <ul style="list-style-type: none"> detail: Show detailed information.

Variable	Description
plan <adom> <start-time> <end-time> <query-tag/norm-qry-hash/sql> <is-fortiview> <max-time-scale>	Plan hcache: <ul style="list-style-type: none"> • adom: The ADOM name. • start-time: The start time (format: yyyy-mm-dd hh:mm:ss). • end-time: The end time (format: yyyy-mm-dd hh:mm:ss). • query-tag/norm-qry-hash/sql: The query tag, normalized query hash, or sql statement. • is-fortiview: Enter 1 for FortiView, or 0 for report. • max-time-scale: Maximum timescale.
rebuild-both <start-time> <end-time>	Rebuild hcache for both report and FortiView. Start and end times are in the format yyyy-mm-dd hh:mm:ss.
rebuild-fortiview <start-time> <end-time>	Rebuild hcache for FortiView only. Start and end times are in the format yyyy-mm-dd hh:mm:ss.
rebuild-report <start-time> <end-time>	Rebuild hcache for report only. Start and end times are in the format yyyy-mm-dd hh:mm:ss.
rebuild-status	Show report hcache rebuild/check status.
show hcache <adom> <id>	Show hcache information. Enter the ADOM name and hcache ID.
show hcache-query <adom> <norm-qry-hash>	Show hcache query information. Enter the ADOM name and the normalized query hash.
show hcache-res-tbl <adom> <res-tbl-id>	Show hcache result table information. Enter the ADOM name and the result table ID.
show time <time> <time> <time> <time>	Show hcache time. Enter up to four timestamps.
status {all <adom> all-summary}	Show detailed hcache information per ADOM, for all ADOMs, or display the summary.

sql process

Use this command to kill or list query processes in the the SQL database.

Syntax

```
diagnose sql process kill <pid>
diagnose sql process list [full]
```

Variable	Description
kill <pid>	Kill a running query.
list [full]	List running query processes.

sql remove

Use this command to remove from the SQL database.

Syntax

```
diagnose sql remove {hcache <adom> <start-time> <end-time> | query-cache | rebuild-db-flag | tmp-table}
```

Variable	Description
{hcache <adom> <start-time> <end-time> query-cache rebuild-db-flag tmp-table}	<p>Remove the selected information:</p> <ul style="list-style-type: none"> hcache: Remove the hcache tables created for the SQL report. <ul style="list-style-type: none"> adom: The ADOM name. start-time: The start time (format: yyyy-mm-dd hh:mm:ss). end-time: The end time (format: yyyy-mm-dd hh:mm:ss). query-cache: Remove the SQL query cache for log search. rebuild-db-flag: Remove the rebuild database flag. The system will exit the rebuild database state. tmp-table: Remove the SQL database temporary tables.

sql show

Use this command to show SQL database information.

Syntax

```
diagnose sql show {db-size | hcache-size | log-filters | log-stfile <device-id> <vdom> | policy-info <adom>}
```

Variable	Description
{db-size hcache-size log-filters log-stfile <device-id> <vdom> policy-info <adom>}	<p>Show the database, hcache size, log filters, or log status file:</p> <ul style="list-style-type: none"> db-size: Show database size. hcache-size: Show hcache size. log-filters: Show log view searching filters. log-stfile: Show logstatus file for the specified device (for HA cluster, input the member's serial number) and VDOM. policy-info: Show policy uuid and name map.

sql status

Use this command to show statuses of the SQL database.

Syntax

```
diagnose sql status {rebuild-adom <adom> | rebuild-db | run_sql_rpt | sqlplugind | sqlreportd}
```

Variable	Description
{rebuild-adom <adom> rebuild-db run_sql_rpt sqlplugind sqlreportd}	Show the status: <ul style="list-style-type: none"> rebuild-adom <adom>: Show SQL log database rebuild status of ADOMs. rebuild-db: Show SQL log database rebuild status. run-sql-rpt: Show run_sql_rpt status. sqlplugind: Show sqlplugind status. sqlreportd: Show sqlreportd status.

sql upload

Use this command to upload sqlplugind messages / pgsvr logs via FTP or SFTP.

Syntax

```
diagnose sql upload {ftp | tftp} <host> <directory> <user_name> <password>
```

Variable	Description
{ftp tftp} <host> <directory> <user_name> <password>	Upload sqlplugind messages / pgsvr logs with FTP or TFTP.

svctools

Import or export the FortiAnalyzer configuration, and run JSON files.

Syntax

```
diagnose svctools export local
diagnose svctools export remote <ip> <string> <username> <password>
diagnose svctools import local name <adom> <integer>
diagnose svctools import remote <ip> <string> <username> <password> <adom> <integer>
diagnose svctools run local filename
diagnose svctools run remote <ip> <string> <username> <password>
```

Variable	Description
export local	Export the configuration locally.

Variable	Description
export remote <ip> <string> <username> <password>	Export the configuration to a remote FTP server.
import local name <adom> <integer>	Import a local configuration from the specified ADOM. Enable or disable upgrade mode.
import remote <ip> <string> <username> <password> <adom> <integer>	Import a remote configuration from an FTP server to the specified ADOM. Enable or disable upgrade mode.
run local filename	Run a local JSON file on the target.
run remote <ip> <string> <username> <password>	Run a remote file from an FTP server.

Example

```
# diagnose svctools export local
Export FortiAnalyzer(121), 1 of 15 ADOM.
Export FortiAuthenticator(137), 2 of 15 ADOM.
Export FortiCache(125), 3 of 15 ADOM.
Export FortiCarrier(117), 4 of 15 ADOM.
Export FortiClient(127), 5 of 15 ADOM.
Export FortiDDoS(135), 6 of 15 ADOM.
Export FortiMail(119), 7 of 15 ADOM.
Export FortiManager(131), 8 of 15 ADOM.
Export FortiNAC(141), 9 of 15 ADOM.
Export FortiProxy(139), 10 of 15 ADOM.
Export FortiSandbox(133), 11 of 15 ADOM.
Export FortiWeb(123), 12 of 15 ADOM.
Export Syslog(129), 13 of 15 ADOM.
Export others(115), 14 of 15 ADOM.
Export root(3), 15 of 15 ADOM.
Exported to /var/tmp/svctools_export
```

system

Use the following commands for system related settings.

system admin-session

Use this command to view and kill log in sessions.

Syntax

```
diagnose system admin-session kill <sid>
diagnose system admin-session list
```

```
diagnose system admin-session status
```

Variable	Description
kill <sid>	Kill a current session. <ul style="list-style-type: none"> <sid>: Session ID
list	List log in sessions.
status	Show the current session.

system disk

Use this command to view disk diagnostic information.



Only `usage` is available on FortiAnalyzer-VM. Other `disk` related commands are only available on the hardware-based FortiAnalyzer.

Syntax

```
diagnose system disk attributes
diagnose system disk delete
diagnose system disk disable
diagnose system disk enable
diagnose system disk health
diagnose system disk info
diagnose system disk errors
diagnose system disk usage <parameter> <parameter> <parameter> <parameter> <parameter>
                        <parameter> <parameter> <parameter> <parameter> <parameter>
```

Variable	Description
attributes	Show vendor specific SMART attributes.
delete	Delete the disk.
disable	Disable SMART support.
enable	Enable SMART support.
health	Show the SMART health status.
info	Show the SMART information.
errors	Show the SMART error logs.
usage <parameter> ... <parameter>	Display the disk usage. Enter a parameter.

Variable	Description	
	Parameter	Description
	-a	Show file sizes.
	-L	Follow all symlinks.
	-H	Follow symlinks on the command line.
	-d N	Limit output to directories (and files with -a) of depth < N.
	-c	Show the grand total.
	-l	Count sizes many times if hard linked.
	-s	Display only a total for each argument.
	-x	Skip directories on different file systems.
	-h	Sizes in human readable format (e.g., 1K 243M 2G).
	-m	Sizes in megabytes.
	-k	Sizes in kilobytes (default).

system export

Use this command to export logs.

Syntax

```

diagnose system export crashlog <ftp server> <username> <password> <directory> <filename>
diagnose system export fmwslog {ftp | sftp} <type> <(s)ftp server> <username> <password>
    <directory> <filename>
diagnose system export raidlog <ftp server> <username> <password> [remote path]
    [filename]
diagnose system export umlog {ftp | sftp} <type> <(s)ftp server> <username> <password>
    <directory> <filename>
diagnose system export upgradelog <ftp server> <username> <password> <directory>
    <filename>
diagnose system export vartmp <ftp server> <username> <password> <directory> <filename>

```

Variable	Description
crashlog <ftp server> <username> <password> <directory> <filename>	Export the crash log.
fmwslog {ftp sftp} <type> <(s)ftp server> <username> <password> <directory> <filename>	Export the web service log files. The type is the log file prefix and can be: SENT, RECV, or TEST.

Variable	Description
raidlog <ftp server> <username> <password> [remote path] [filename]	Export the RAID log. This command is only available on devices that support RAID.
umlog {ftp sftp} <type> <(s)ftp server> <username> <password> <directory> <filename>	Export the update manager and firmware manager log files. The type options are: fdslinkd, fctlinkd, fgdlinkd, fgdsvr, update, service, misc, umad, and fwmlinkd
upgradelog <ftp server> <username> <password> <directory> <filename>	Export the upgrade error log.
vartmp <ftp server> <username> <password> <directory> <filename>	Export the system log files in /var/tmp.

system flash

Use this command to diagnose the flash memory.

Syntax

```
diagnose system flash list
```

Variable	Description
list	List flash images. The information displayed includes the image name, version, total size (KB), used (KB), percent used, boot image, and running image.

system fsck

Use this command to check and repair the file system, and to reset the disk mount count.

Syntax

```
diagnose system fsck harddisk
diagnose system fsck reset-mount-count
```

Variable	Description
harddisk	Check and repair the file system, then reboot the system.
reset-mount-count	Reset the mount-count of the disk on the next reboot.

system geoip

Use these commands to get geoip information.

FortiAnalyzer uses a [MaxMind GeoLite](#) database of mappings between geographic regions and all public IPv4 addresses that are known to originate from them.

Syntax

```
diagnose system geoip dump
diagnose system geoip info
diagnose system geoip ip <ip>
```

Variable	Description
dump	Display all geographic IP information.
info	Display a brief geography IP information.
ip <ip>	Find the specified IP address' country.

Example

Find the country of the IP address 4.3.2.1:

```
FAZVM64 # diagnose system geoip ip 4.3.2.1
4.3.2.1 : US - United States
```

system geoip-city

Use these commands to get geographic IP information at a city level.

Syntax

```
diagnose system geoip-city info
diagnose system geoip-city ip <ip>
```

Variable	Description
info	Display geographic IP information.
ip <ip>	Find the specified IP address' city.

system interface

Use this command to diagnose the interface.

Syntax

```
diagnose system interface segmentation-offload <intf-name> <action>
```

Variable	Description
segmentation-offload <intf-name> <action>	Print/set segmentation-offload for all interfaces: <ul style="list-style-type: none"><intf-name>: Enter the interface name (or enter <code>all</code> for all interfaces)<action>: Enter one of <code>show/on/off</code> to show or switch on/off interfaces

system mapserver

Use this command to access the map server information.

Syntax

```
diagnose system mapserver get
diagnose system mapserver reset
diagnose system mapserver set <url>
diagnose system mapserver test
```

Variable	Description
get	Get the current map server.
reset	Reset the map server session.
set <url>	Set the map server. Enter the map server URL.
test	Test the map server connection.

system ntp

Use this command to list NTP server information.

Syntax

```
diagnose system ntp status
```

Variable	Description
status	List NTP server information.

system print

Use this command to print server information.

Syntax

```
diagnose system print connector [adom] <server_type> <server> <tag>
diagnose system print cpuinfo
diagnose system print df [arg0] [arg1] [arg2] .... [arg9]
diagnose system print hosts
diagnose system print interface <interface>
diagnose system print loadavg
diagnose system print netstat
diagnose system print partitions
diagnose system print route
diagnose system print rtcache
diagnose system print slabinfo
diagnose system print sockets
diagnose system print uptime
```

Variable	Description
connector [adom] <server_type> <server> <tag>	Print connector information. Enter the ADOM name, or Global, the server type (pxGrid, clearpass, or nsx), and then the server name.
cpuinfo	Print the CPU information.
df [arg0] [arg1] [arg2] [arg9]	Print the file system disk space usage. Optionally, enter arguments.
hosts	Print the static table lookup for host names.
interface <interface>	Print the specified interface's information.
loadavg	Print the average load of the system.
netstat	Print the network statistics for active Internet connections (servers and established).
partitions	Print the disk partition information.
route	Print the main route list.
rtcache	Print the contents of the routing cache.
slabinfo	Print the slab allocator statistics.
sockets	Print the currently used socket ports.
uptime	Print how long the system has been running.

system process

Use this command to view and kill processes.

Syntax

```
diagnose system process fdlist <pid>
diagnose system process kill -<signal> <pid>
diagnose system process killall {Scriptmgr | deploymgr | fgfm}
diagnose system process list
```

Variable	Description
fdlist <pid>	List all file descriptors that the process is using. <ul style="list-style-type: none"> <pid>: Process ID
kill -<signal> <pid>	Kill a process: <ul style="list-style-type: none"> -<signal>: Signal name or number, such as -9 or -KILL <pid>: Process ID
killall {Scriptmgr deploymgr fgfm}	Kill all the related processes.
list	List all processes running on the FortiAnalyzer. The information displayed includes the PID, user, VSZ, stat, and command.

system raid

Use this command to view RAID information.



This command is only available on hardware-based FortiAnalyzer models that support RAID.

Syntax

```
diagnose system raid cc <rate> <delay>
diagnose system raid hwinfo
diagnose system raid status
```

Variable	Description
cc <rate> <delay>	Show/Set RAID consistency check rate (1-100%, 0 = no change) and delay (1-8760 hours, 0 = no change).
hwinfo	Show RAID controller hardware information.
status	Show RAID status.

system route

Use this command to help diagnose routes. The listed information includes the destination IP, gateway IP, netmask, flags, metric, reference, use, and interface for each IPv4 route.

The following flags can appear in the route list table:

- U*: the route is up
- G*: the route is to a gateway
- H*: the route is to a host rather than a network

- *D*: the route was dynamically created by a redirect
- *M*: the route was modified by a redirect

Syntax

```
diagnose system route list
```

system route6

Use this command to help diagnose routes. The listed information includes the destination IP, gateway IP, netmask, flags, metric, reference, use, and interface for each IPv6 route.

For a list of flags that can appear in the route6 list table, see information for the `diagnose system route list` command above.

Syntax

```
diagnose system route6 list
```

system server

Use this command to start the FortiAnalyzer server.

Syntax

```
diagnose system server start
```

test

Use the following commands to test the FortiAnalyzer.

test application

Use this command to test application daemons. Enter an unassigned integer value to see the available options for each command.

Syntax

```
diagnose test application apiproxyd <integer> <integer> ... <integer>
diagnose test application archd <integer> <integer> ... <integer>
diagnose test application clusterd <integer> <integer> ... <integer>
diagnose test application execcmd <integer> <integer> ... <integer>
diagnose test application fabricsyncd <integer> <integer> ... <integer>
diagnose test application fazcfgd <integer> <integer> ... <integer>
```

```

diagnose test application fazmaild <integer> <integer> ... <integer>
diagnose test application faznotify <integer> <integer> ... <integer>
diagnose test application fazsvcd <integer> <integer> ... <integer>
diagnose test application fazwatchd <integer> <integer> ... <integer>
diagnose test application filefwd <integer> <integer> ... <integer>
diagnose test application fileparsed <integer> <integer> ... <integer>
diagnose test application fortilogd <integer> <integer> ... <integer>
diagnose test application logfiled <integer> <integer> ... <integer>
diagnose test application logfwd <integer> <integer> ... <integer>
diagnose test application log-fetchd <integer> <integer> ... <integer>
diagnose test application miglogd <integer> <integer> ... <integer>
diagnose test application oftpd <integer> <integer> ... <integer>
diagnose test application rptchkd <integer> <integer> ... <integer>
diagnose test application scansched <integer> <integer> ... <integer>
diagnose test application siemagentd <integer> <integer> ... <integer>
diagnose test application siemdbd <integer> <integer> ... <integer>
diagnose test application snmpd <integer> <integer> ... <integer>
diagnose test application sqllogd <integer> <integer> ... <integer>
diagnose test application sqlplugind <integer> <integer> ... <integer>
diagnose test application sqlreportd <integer> <integer> ... <integer>
diagnose test application sqlrptcached <integer> <integer> ... <integer>
diagnose test application syncsched <integer> <integer> ... <integer>
diagnose test application uploadd <integer> <integer> ... <integer>

```

Variable	Description
apiproxyd <integer> ...	API proxy daemon test usage: <ul style="list-style-type: none"> 1: show PID 2: show statistics and state 20: fsa tracer log request 21: fsa tracer log request 99: restart daemon
archd <integer> ...	Archd daemon test usage: <ul style="list-style-type: none"> 1: usage 2: display content subdir info file 3: force scan to archive ips files 4: force preen content files 99: restart daemon
clusterd <integer> ...	Clusterd daemon test usage: <ul style="list-style-type: none"> 1: Daemon info (PID, meminfo, backtrace ...) 2: Thread pool status 3: Log Cluster core 4: Devices cache module 5: Logging Topology module 6: Avatar uploading module 7: Meta-CSF uploading module 8: Meta-InterfaceRole module 9: Tunnel module 10: oftpd file fwd module 11: Service module

Variable	Description
	<ul style="list-style-type: none"> • 97: HA module • 98: Monitor status • 99: Restart clusterd • 100: Restart clusterd and clusterd-monitor • 102: Various tests • 103: generate core dump (on or off) when cluster.monitor kills cluster.main
execcmd <integer> ...	Execcmd daemon test usage: <ul style="list-style-type: none"> • 1: show PID • 2: show statistics and state • 3: reset statistics and state • 4: show statistics of cmd tool • 5: reset statistics of cmd tool • 99: restart daemon
fabricsyncd <integer> ...	Fabricsyncd daemon test usage.
fazcfgd <integer> ...	Fazcfg daemon test usage: <ul style="list-style-type: none"> • 1: Daemon info (PID, meminfo, backtrace ...) • 2: show statistics • 3: show merged ca info • 40: DVM cache diag info • 41: CSF diag info • 42: IntfRole diag info • 43: reload csf info in devtable • 44: show log device group stats • 45: check log device group • 46: metadata table diag info [sub-module] • 48: test update link prefixes file • 49: test update webfilter categories description file • 50: test get app icon • 51: test update app logo files • 52: dvm call stats • 53: dvm call stats clear • 54: check ips/app meta-data update • 55: log disk readahead get • 56: log disk readahead toggle • 57: fix redis service • 58: check redis service • 59: test update faz license • 60: test fortigate restful api • 65: log aggregation server stats • 66: log aggregation server stats toggle (debug only) • 67: test redis security connect [port] [key] [value]

Variable	Description
	<ul style="list-style-type: none"> 82: list avatar meta-data 83: rebuild avatar meta-data table 84: rebuild ips meta-data table 85: rebuild app meta-data table 86: rebuild FortiClient Vulnerability meta-data table 88: update ffdb meta-data 90: use built-in TIDB package and disable updating it 91: enable updating TIDB package 92: disable updating TIDB package 93: switch on/off adom default report schedule 94: switch on/off report schedule by name 97: set 'force_restore_data' flag for clickhouse start 99: restart daemon
fazmaild <integer> ...	<p>Fazmaild daemon test usage:</p> <ul style="list-style-type: none"> 1: show PID and daemon status 2: show runtime status 90: pause sending mail 91: resume sending mail 99: restart fazmaild daemon
faznotify <integer> ...	<p>Faznotify daemon test usage:</p> <ul style="list-style-type: none"> 1: Daemon info (PID, meminfo, backtrace ...) 2: show faznotify statistics [clear] 10: send a faznotify <adom> <id> <send-data> 20: show active channel 29: delete active channel <adom> <id> 30: pause active channel <seconds> 99: restart
fazsvcd <integer> ...	<p>Fazsvcd daemon test usage:</p> <ul style="list-style-type: none"> 1: Daemon info (PID, meminfo, backtrace ...) 2: show daemon stats and status 3: list async search threads 4: dump async search slot info 5: show cache builder stats 6: dump cache builder playlist 7: dump log search filters 10: show database log stats aggregated per day 11: show received log stats aggregated per day 20: show avatar request stats 50: enable or disable cache builder 51: enable or disable auto custom index 57: Fazbroker stats 58: reset Fazbroker stats

Variable	Description
	<ul style="list-style-type: none"> • 60: rawlog idx cache test • 61: logbrowse cache stats • 62: FortiView Session Stats • 70: show stats for device vdom cache • 71: show stats for remote fortiview and reports • 72: show filterable and sortable fields for fortiview. <v3.0 view name> • 75: data masking test: <passwd> <plaint test> <1 0 (high secure)> [do_unmasking] • 76: fazsvcd fabric service diagnostics • 99: restart daemon • 100: log FAZ debugs • 101: Close FAZ debug log • 200: gui api test • 201: diag for jsonrpc ..
fazwatchd <integer> ...	<p>Fazwatchd daemon test usage:</p> <ul style="list-style-type: none"> • 1: show process summary and report stats • 2: show playbook stats • 4: show nac asset stats • 5: show playbook task log • 6: show ha command execution stats • 7: show casb metadata stats • 8: show ems metadata stats • 9: show pgsvr.log monitor stats • 99: restart daemon
filefwd <integer> ...	<p>Filefwd daemon test usage:</p> <ul style="list-style-type: none"> • 1: show daemon PID • 2: show daemon stats • 3: show threads stats • 99: restart daemon
fileparsed <integer> ...	<p>Fileparsed daemon test usage:</p> <ul style="list-style-type: none"> • 1: show PID • 2: show statistics and state • 3: show devtable local cache status • 4: reload devtable local cache. • 11: show FortiGate interface cache status • 12: show FortiGate interface parsers status • 13: show FortiGate interface archived files disk usage • 14: show FortiGate interface archived files retention days • 15: show FortiGate interface info • 16: show total number of interfaces trimmed from database • 17: show FortiGate policy files process status • 18: show total number of policy records in database • 98: rebuild FortiGate interface SQL tables

Variable	Description
	<ul style="list-style-type: none"> • 99: restart daemon
fortilogd <integer> ...	<p>Fortilogd Diag test usage:</p> <ul style="list-style-type: none"> • 1: Daemon info (PID, meminfo, backtrace ...) • 2: dump message status • 3: logstat status • 4: client devices status • 5: print log received • 6: switch on/off debug messages • 7: log forwarding prep status • 8: show logUID info • 9: device log cache reloading status • 10: dz_client cache status • 11: file stats • 12: stop/restart receiving logs • 14: show cached adom lograte status • 15: show cached adom log volume status • 16: show appevent logs receiving info • 17: show logging rate of the system and per-device • 90: show or set fortilogd working status • 95: show runtime logs. option format: pid=0:current,-1:all,PID duration=DURA filter=STR • 98: memory check • 99: restart fortilogd
logfiled <integer> ...	<p>Logfile daemon test usage:</p> <ul style="list-style-type: none"> • 1: Daemon info (PID, meminfo, backtrace ...) • 2: show statistics and state • 4: show ADOM statistics • 5: show device statistics • 6: show auto-del statistics • 7: show log file disk usage • 8: update log file disk usage • 9: show inode usage • 10: enable or disable debug filterof device and vdom • 11: du cache diag commands • 12: force to checkthe oldest log litime when trim log files. • 90: reset statistics and state • 91: force to preen content files info • 99: restart daemon
logfwd <integer> ...	<p>Logfwd daemon test usage:</p> <ul style="list-style-type: none"> • 1: Daemon info (PID, meminfo, backtrace ..) • 2: Dump thread-pool status • 3: Dump log-forward configurations

Variable	Description
	<ul style="list-style-type: none"> • 4: Dump log-forwarding status • 5: Overall and converter stats • 6: Dump HA CID info • 7: show runtime logs. option format: pid=0:current,-1:all,PID duration=DURA filter=STR • 8: show cfile list status [all: for all cfiles] • 9: show max duration of loss in memory mode, 120 seconds default, 0 to disable memory mode • 10: Force logfwd to run in disk mode [1:enable, 0:disable] • 97: memory check • 98: Reset log-forwarding stats • 99: Restart logfwd
log-fetchd <integer> ...	Log-fetch daemon test usage: <ul style="list-style-type: none"> • 1: show PID • 2: show states • 3: show running sessions • 99: restart the daemon
miglogd <integer> ...	Miglogd daemon test usage: <ul style="list-style-type: none"> • 1: show PID • 2: dump memory pool • 99: restart daemon
oftpd <integer> ...	Oftpd daemon test usage: <ul style="list-style-type: none"> • 1: show PID • 2: show statistics and state • 3: show connected device name and IP • 4: show detailed session state • 5: show oftp request statistics • 6: show cmdb device cache • 7: show logfwd thread stats • 8: show tasklist statistics • 9: show unreg dev cache • 10: log cluster bridge stats • 12: show HA group cache • 13: show file fwd stats • 14: show fct software inventory cache • 15: show fgt interface stats • 16: show fos-auto device dump. [dev] to dump device list • 17: show device logging rate & rate-limit. [enable] to force tracking log-rate or [disable] to track only rate-limited devices. [config] to show config • 18: show fgt policy info, [dev] to dump device list • 21: dump oftp-restapi-sched stats • 22: dump oftp-restapi-sched status • 23: dump oftp csf member status

Variable	Description
	<ul style="list-style-type: none"> • 30: dump csf groups data in all adoms in json string • 31: show csf groups update stats • 32: reschedule all restapi task for designated devid • 40: test loading a CA cert from local path • 50: display logtypes for all devid • 60: display login requests stats • 80: set region • 90: reload un-reg device tree • 91: delete designated csf group • 92: reload reg dev cache • 95: debug output • 99: restart daemon
rptchkd <integer> ...	<p>Sqlrptcache daemon test usage:</p> <ul style="list-style-type: none"> • 1: show PID • 2: show statistics and state • 3: reset statistics and state • 4: list adoms • 6: list schedules • 55: re-check an adom • 99: restart daemon • 910: enable rptchkd • 911: disable rptchkd
scansched <integer> ...	<p>Scansched daemon test usage:</p> <ul style="list-style-type: none"> • 1: show PID • 2: show statistics and state • 3: reset statistics and state • 11: show ioc-rescan task status • 99: restart daemon
siemagentd <integer> ...	<p>Siemagentd daemon test usage:</p> <ul style="list-style-type: none"> • 1: show PID • 2: show daemon statistics • 3: show daemon worker statistics • 4: show daemon worker status stats • 5: show supported device-log types • 11: worker process run • 12: worker process suspend • 13: worker process exit • 20: show the siem stream storage info • 21: show the latest siem stream submitted in redis • 99: restart daemon • 200: diag for log based alert (event mgmt) • 205: diag for endpoint and enduser

Variable	Description
siemdbd <integer> ...	<p>Siemdbd daemon test usage:</p> <ul style="list-style-type: none"> • 1: Daemon info (PID, meminfo, backtrace ...) • 2: show statistics and state • 3: show running processes • 4: show writers info • 5: show splitter info • 6: show Adom database info • 7: show trimmer info • 8: show the shared Materialized View disk usage info • 9: set/reset max memory usage ratio • 10: add or drop skip indices on SIEM table • 41: show writer 1 info • 42: show writer 2 info • 43: show writer 3 info • 97: clear redis stream • 99: restart daemon
snmpd <integer> ...	<p>SNMP daemon test usage:</p> <ul style="list-style-type: none"> • 1: display daemon pid • 2: display snmp statistics • 3: clear snmp statistics • 4: generate test trap (cpu high) • 5: generate test traps (log alert, rate, data rate) • 6: generate test traps (licensed gb/day, device quota) • 99: restart daemon
sqllogd <integer> ...	<p>SqlLog daemon test usage:</p> <ul style="list-style-type: none"> • 1: Daemon info (PID, meminfo, backtrace ...) • 2: show statistics and state • 3: show worker init state • 4: show worker thread info • 5: show log device scan info, optionally filter by <devid> • 7: show ADOM device list by <adom-name> • 8: show logUID info • 9: show ADOM scan sync info, optionally filter by <adom> • 10: show FortiClient dev to sql-ID (sID) map • 11: show devtable cache info • 12: show intfrole cache info • 41: show worker 1 info • 51: show worker 1 registered log devices • 61: show worker 1 open log file cache • 70: show sql database building progress • 71: show the progress of upgrading log files into per-vdom storage • 72: run the upgrading log files into per-vdom storage

Variable	Description
	<ul style="list-style-type: none"> • 80: show daemon status flags • 81: show debug zone devices status • 82: show all adoms with member devices or filter by <adom-name> • 83: show all registered logdevs • 84: show all unreg logdevs • 85: show fazid map stats • 91: diag worker devvd loadbalance • 95: request to rebuild SQL database for local event logs • 96: resend all pending batch files to sqlplugind • 97: rebuilding warm restart • 98: set worker assignment to policy 'round-robin' or 'adom-affinity', daemon will restart on policy change. • 99: restart daemon • 200: diag for log based alert (event mgmt) .. • 201: diag for utmref cache .. • 202: diag for fgt-fct corelation .. • 203: diag for logstat .. • 204: diag for loC .. • 205: diag for endpoint and enduser .. • 206: diag for ueba .. • 207: diag for FSA scan session .. • 208: diag for audit report event process .. • 209: diag for shadow it info .. • 221: estimated browsing time stats • 222: fsa devmap cache info • 224: fgt lograte cache info • 225: dump enum field error cache • 226: reset enum field error cache • 227: dump tz field error cache • 228: reset tz field error cache
sqlplugind <integer> ...	<p>Sqlplugind daemon test usage:</p> <ul style="list-style-type: none"> • 1: Daemon info (PID, meminfo, backtrace ...) • 2: show daemon stats • 3: show SIEM table stats • 4: show table compressor stats • 5: show table compressor Adom stats • 6: show table slow upgrade info • 91: scan hcache query templates and clean up unused • 98: scan and clean zombie cstore files • 99: restart daemon
sqlreportd <integer> ...	<p>Sqlreportd daemon test usage:</p> <ul style="list-style-type: none"> • 1: Daemon info (PID, meminfo, backtrace ...) • 2: show daemon stats

Variable	Description
	<ul style="list-style-type: none"> • 3: show restorable table schema • 4: show restorable table status • 99: restart daemon
sqlrptcached <integer> ...	Sqlrptcache daemon test usage: <ul style="list-style-type: none"> • 1: Daemon info (PID, meminfo, backtrace ...) • 2: show statistics and state • 3: reset statistics and state • 5: dump auto-cache charts • 99: restart daemon
syncsched <integer> ...	Syncsched daemon test usage: <ul style="list-style-type: none"> • 1: Daemon info (PID, meminfo, backtrace ...) • 2: show report nodes states • 3: show report syncing state • 4: show ha sync peers • 5: reset ha sync queue • 6: show ha elog sync • 10: sync reports with peer • 11: fsync stat • 12: fsync reload • 13: trim sync dir stat • 99: restart daemon
uploadadd <integer> ...	Uploadadd daemon test usage: <ul style="list-style-type: none"> • 1: Daemon info (PID, meminfo, backtrace ...) • 2: show statistics and state • 3: reset statistics and state • 4: show uploadadd queues content • 5: show upload server state • 50: clear log queue [mirror server1] • 51: clear log queue [mirror server2] • 52: clear log queue [mirror server3] • 53: clear log queue [backup] • 54: clear log queue [original request] • 55: clear log queues [all] • 56: clear report queue • 60: cloud storage bget backlog info • 61: cloud storage get setting pending info <setting name> • 62: cloud storage test connector <connector> <remote path> • 63: cloud storage get usage info • 99: restart daemon

test connection

Test the connection to the mail server and syslog server.

Syntax

```
diagnose test connection fortianalyzer <ip>
diagnose test connection mailserver <server-name> <mail-from> <mail-to>
diagnose test connection syslogserver <server-name>
```

Variable	Description
fortianalyzer <ip>	Test the connection to the FortiAnalyzer.
mailserver <server-name> <mail-from> <mail-to>	Test the connection to the mail server.
syslogserver <server-name>	Test the connection to the syslog server.

test policy-check

Check policy consistency.

Syntax

```
diagnose test policy-check flush
diagnose test policy-check list
```

Variable	Description
flush	Flush all policy check sessions.
list	List all policy check sessions.

test search

Test the search daemon.

Syntax

```
diagnose test search flush
diagnose test search list
```

Variable	Description
flush	Flush all search sessions.
list	List all search sessions.

test sftp

Use this command to test the secure file transfer protocol (SFTP) scheduled backup.

Syntax

```
diagnose test sftp auth <sftp server> <username> <password> <directory>
```

Variable	Description
<sftp server>	SFTP server IP address.
<username>	SFTP server username.
<password>	SFTP server password.
<directory>	The directory on the SFTP server where you want to put the file (default = /).

upload

Use the following commands for upload related settings.

upload clear

Use this command to clear the upload request.

Syntax

```
diagnose upload clear log {all | backup | mirror 1 | mirror 2 | mirror 3 | original}
diagnose upload clear report
```

Variable	Description
log {all original backup mirror 1 mirror 2 mirror 3}	<p>Clear log uploading requests.</p> <ul style="list-style-type: none">• all: Clear all log uploading requests.• backup: Clear log uploading requests in the backup queue.• mirror 1: Clear log uploading requests in the mirror queue for server 1.• mirror 2: Clear log uploading requests in the mirror queue for server 2.• mirror 3: Clear log uploading requests in the mirror queue for server 3.• original: Clear log uploading requests in the original queue.
report	Clear all report upload requests.

upload status

Use this command to get the running status on files in the upload queue.

Syntax

```
diagnose upload status
```

vpn

Use this command to flush SAD entries and list tunnel information.

Syntax

```
diagnose vpn tunnel flush-SAD
diagnose vpn tunnel list
```

Variable	Description
flush-SAD	Flush the SAD entries.
list	List tunnel information.

get

The `get` commands display a part of your FortiAnalyzer unit's configuration in the form of a list of settings and their values.



Although not explicitly shown in this section, for all `config` commands there are related `get` and `show` commands that display that part of the configuration. `get` and `show` commands use the same syntax as their related `config` command, unless otherwise specified.



CLI commands and variables are case sensitive.

The `get` command displays all settings, including settings that are in their default state.

Unlike the `show` command, `get` requires that the object or table whose settings you want to display are specified, unless the command is being used from within an object or table.

For example, at the root prompt, this command would be valid:

```
get system status
```

and this command would not:

```
get
```

fmupdate analyzer	fortirecorder camera	system fips	system password-policy
fmupdate av-ips	fortirecorder global	system fortiview	system performance
fmupdate custom-url-list	fortirecorder schedule	system global	system report
fmupdate disk-quota	system admin	system ha	system route
fmupdate fct-services	system alert-console	system interface	system route6
fmupdate fds-setting	system alertemail	system locallog	system saml
fmupdate fwm-setting	system alert-event	system log	system sniffer
fmupdate multilayer	system auto-delete	system log-fetch	system snmp
fmupdate publicnetwork	system backup	system log-forward	system soc-fabric
fmupdate server-access-priorities	system central-management	system log-forward-service	system sql
fmupdate server-override-status	system certificate	system loglimits	system status
fmupdate service	system connector	system mail	system syslog

fmupdate web-spam	system dns	system metadata	system web-proxy
	system docker	system ntp	

fmupdate analyzer

Use this command to view the virus report to FDS.

Syntax

```
get fmupdate analyzer virusreport
```

fmupdate av-ips

Use these commands to view AV/IPS update settings.

Syntax

```
get fmupdate av-ips advanced-log
get fmupdate av-ips web-proxy
```

Example

This example shows the output for `get fmupdate av-ips web-proxy`:

```
ip : 0.0.0.0
ip6 : ::
mode : proxy
password : *
port : 80
status : disable
username : (null)
```

fmupdate custom-url-list

Use this command to view the custom URL database.

Syntax

```
get fmupdate custom-url-list
```

fmupdate disk-quota

Use this command to view the disk quota for the update manager.

Syntax

```
get fmupdate disk-quota
```

Example

This example shows the output for `get fmupdate disk-quota`:

```
value : 51200
```

fmupdate fct-services

Use this command to view FortiClient update services configuration.

Syntax

```
get fmupdate fct-services
```

Example

This example shows the output for `get fmupdate fct-services`:

```
status : enable  
port : 80
```

fmupdate fds-setting

Use this command to view FDS parameters.

Syntax

```
get fmupdate fds-setting
```

Example

This example shows the output for `get fmupdate fds-setting`:

```
User-Agent : Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)  
fds-clt-ssl-protocol: tlsv1.2
```

```
fds-ssl-protocol : tlsv1.2
fmtr-log : info
fortiguard-anycast : disable
fortiguard-anycast-source: fortinet
linkd-log : info
max-av-ips-version : 20
max-work : 1
push-override:
push-override-to-client:
send_report : enable
send_setup : disable
server-override:
system-support-faz :
system-support-fct :
system-support-fdc :
system-support-fgt :
system-support-fml :
system-support-fsa :
system-support-fts :
umsvc-log : info
unreg-dev-option : add-service
update-schedule:
    time: 00:10 wanip-query-mode : disable
```

fmupdate fwm-setting

Use this command to view firmware management settings.

Syntax

```
get fmupdate fwm-setting
```

Example

This example shows the output for `get fmupdate fwm-setting`:

```
auto-scan-fgt-disk : enable
check-fgt-disk : enable
fds-failover-fmg : enable
fds-image-timeout : 1800
immx-source : fmg
log : fwm_dm
multiple-steps-interval: 60
retry-interval : 60
retry-max : 10
upgrade-timeout:
```

fmupdate multilayer

Use this command to view multilayer mode configuration.

Syntax

```
get fmupdate multilayer
```

fmupdate publicnetwork

Use this command to view public network configuration.

Syntax

```
get fmupdate publicnetwork
```

fmupdate server-access-priorities

Use this command to view server access priorities.

Syntax

```
get fmupdate server-access-priorities
```

Example

This example shows the output for `get fmupdate server-access-priorities`:

```
access-public : disable
av-ips : disable
private-server:
web-spam : enable
```

fmupdate server-override-status

Use this command to view server override status configuration.

Syntax

```
get fmupdate server-override-status
```

fmupdate service

Use this command to view update manager service configuration.

Syntax

```
get fmupdate service
```

Example

This example shows the output for `get fmupdate service`:

```
avips : enable
```

fmupdate web-spam

Use these commands to view web spam configuration.

Syntax

```
get fmupdate web-spam fgd-setting
get fmupdate web-spam web-proxy
```

Example

This example shows the output for `get fmupdate web-spam web-proxy`:

```
ip : 0.0.0.0
ip6 : ::
mode : proxy
password : *
port : 80
status : disable
username : (null)
```

fortirecorder camera

Use these commands to view camera devices, profiles, and video profiles information.

Syntax

```
get fortirecorder camera devices [camera name]
get fortirecorder camera profile [profile name]
get fortirecorder camera video profile [profile name]
```


Examples

This example shows the output for `get fortirecorder camera video profile low-resolution`:

```
name           : low-resolution
video-resolution : low
video-codec     : default
video-fps      : 30
video-bitrate-mode : variable
video-quality   : low
audio          : disable
```

fortirecorder global

Use this command to view global FortiRecorder information.

Syntax

```
get fortirecorder global
```

Example

```
# get fortirecorder global
camera-key       : *
public-address   : (null)
public-ftp-port  : 21
public-http-port : 80
public-https-port : 443
public-notify-http-port: 3011
public-notify-tcp-port: 3010
public-rtsp-port : 554
```

fortirecorder schedule

Use this command to view FortiRecorder schedule information.

Syntax

```
get fortirecorder schedule object [schedule]
```

Example

```
# get fortirecorder schedule object Always
name           : Always
description    : Default always schedule
```

```
type           : recurring
all-day        : enable
days          : su mo tu we th fr sa
```

system admin

Use these commands to view admin configuration.

Syntax

```
get system admin group [group name]
get system admin ldap [server entry name]
get system admin profile [profile ID]
get system admin radius [server entry name]
get system admin setting
get system admin tacacs [server entry name]
get system admin user [username]
```

Example

This example shows the output for `get system admin setting`:

```
access-banner : disable
admin-https-redirect: enable
admin-login-max : 256
admin_server_cert : server.crt
auth-addr : (null)
auth-port : 443
banner-message : (null)
fsw-ignore-platform-check: disable
gui-theme : blue
http_port : 80
https_port : 443
idle_timeout : 900
idle_timeout_api : 900
idle_timeout_gui : 900
idle_timeout_sso : 900
objects-force-deletion: enable
preferred-fgfm-intf : (null)
shell-access : disable
show-add-multiple : disable
show-checkbox-in-table: disable
show-device-import-export: disable
show-fct-manager : disable
show-hostname : disable
show-log-forwarding : enable
unreg_dev_opt : add_allow_service
webadmin_language : auto_detect
```

system alert-console

Use this command to view the alert console settings.

Syntax

```
get system alert-console
```

Example

This example shows the output for `get system alert-console`:

```
period : 7
severity-level : emergency
```

system alertemail

Use this command to view alert email settings.

Syntax

```
get system alertemail
```

Example

This example shows the output for `get system alertemail`:

```
authentication : enable
fromaddress : (null)
fromname : (null)
smtppassword : *
smtpport : 25
smtpserver : (null)
smtpuser : (null)
```

system alert-event

Use this command to view alert event information.

Syntax

```
get system alert-event [alert name]
```

Example

This example shows the output for an alert event named `Test` that has default values:

```
name : Test
alert-destination:
enable-generic-text : disable
enable-severity-filter: disable
event-time-period : 0.5
generic-text : (null)
num-events : 1
severity-filter : high
severity-level-comp : =
severity-level-logs : no-check
```

system auto-delete

Use this command to view automatic deletion policies for logs, reports, DLP files, and quarantined files.

Syntax

```
get system auto-delete
```

system backup

Use the following commands to view backups:

Syntax

```
get system backup all-settings
get system backup status
```

Example

This example shows the output for `get system backup status`:

```
All-Settings Backup
  Last Backup: Tue Sep 29 08:03:35 2020
  Next Backup: N/A
```

system central-management

Use this command to view the central management configuration.

Syntax

```
get system central-management
```

Example

This example shows the output for `get system central-management`:

```
type : fortimanager
allow-monitor : enable
fmng : (null)
enc-algorithm : default
authorized-manager-only: enable
serial-number :
```

system certificate

Use these commands to view certificate configuration.

Syntax

```
get system certificate ca [certificate name]
get system certificate crl [crl name]
get system certificate local [certificate name]
get system certificate oftp [certificate name]
get system certificate remote [certificate name]
get system certificate ssh [certificate name]
```

Example

This example shows the output for `get system certificate local Fortinet_Local`:

```
name : Fortinet_Local
password : *
comment : Default local certificate
private-key :
certificate :
  Subject: C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiAnalyzer, CN
           = FAZ-VM0000000001, emailAddress = support@fortinet.com
  Issuer: C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate
           Authority, CN = fortinet-subca2001, emailAddress = support@fortinet.com
  Valid from: 2017-08-30 26:03:83 GMT
  Valid to: 2056-01-19 33:14:77 GMT
  Fingerprint: 68:--:--:--:--:--:--:--:--:--:--:--:--:--:--:--:7C
  Root CA: No
  Version: 3
  Serial Num:
    38:f9
  Extensions:
    Name: X509v3 Subject Key Identifier
    Critical: no
```

```
Content:  
EC:--:--:--:--:--:--:--:--:--:--:--:--:94  
Name: X509v3 Authority Key Identifier  
Critical: no  
Content:  
keyid:98:--:--:~::~:~::~:~::~:~::~:~::~:~::~:~::~:~::~:~::~:D7  
DirName:/C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=Certificate Authority/CN=fortinet-  
ca2/emailAddress=support@fortinet.com  
serial:20:01  
Name: X509v3 Basic Constraints  
Critical: yes  
Content:  
CA:FALSE  
Name: X509v3 Key Usage  
Critical: yes  
Content:  
Digital Signature
```

csr :

system connector

Use this command to view FSSO connector refresh intervals, in seconds.

Syntax

```
get system connector
```

Example

This example shows the output for `get_system_connector`:

```
conn-refresh-interval : 300
fsso-refresh-interval: 180
fsso-sess-timeout : 300
px-svr-timeout : 300
```

system dns

Use this command to view DNS settings.

Syntax

```
get system dns
```

Example

This example shows the output for `get system dns`:

```
primary : 111.11.111.11
secondary : 111.11.111.12
ip6-primary : ::
ip6-secondary : ::
```

system docker

Use this command to view Docker and management extension statuses.

Syntax

```
get system docker
```

Example

This example shows the output for `get system docker`:

```
status : disable
cpu : 50
mem : 50
default-address-pool_base : 172.17.0.0 255.255.0.0
default-address-pool_size : 24
docker-user-login-max: 32
```

system fips

Use this command to view FIPS settings.

Syntax

```
get system fips
```

Example

This example shows the output for `get system fips`:

```
entropy-token : enable
re-seed-interval : 1440
```

system fortiview

Use this command to view the FortiView settings.

Syntax

```
get system fortiview auto-cache
get system fortiview settings
```

Example

This example shows the output for `get system fortiview auto-cache`:

```
aggressive-fortiview: disable
interval : 168
status : enable
```

system global

Use this command to view global system settings.

Syntax

```
get system global
```

Example

This example shows the output for `get system global`:

```
admin-lockout-duration: 60
admin-lockout-threshold: 3
adom-mode : normal
adom-status : disable
backup-compression : normal
backup-to-subfolders: disable
clone-name-option : default
clt-cert-req : disable
console-output : standard
contentpack-fgt-install : disable
country-flag : enable
create-revision : disable
daylightsavetime : enable
default-logview-auto-completion : enable
default-search-mode : filter-based
detect-unregistered-log-device: enable
device-view-mode : regular
dh-params : 2048
disable-module : fortirecorder ai
```



```
enc-algorithm : high
fgfm-local-cert : (null)
fgfm-ssl-protocol : tlsv1.0
fortirecorder-disk-quota: 3072
gui-curl-timeout: 30
gui-polling-interval: 5
ha-member-auto-grouping: enable
hostname : FAZVM64
language : english
latitude : (null)
ldap-cache-timeout : 86400
ldapconntimeout : 60000
log-checksum : none
log-forward-cache-size: 30
log-mode : analyzer
longitude : (null)
max-aggregation-tasks: 0
max-running-reports : 1
multiple-steps-upgrade-in-autolink: disable
no-copy-permission-check: disable
normalized-intf-zone-only: disable
object-revision-db-max : 100000
object-revision-mandatory-note : enable
object-revision-object-max : 100
object-revision-status : enable
oftp-ssl-protocol : tlsv1.2
policy-object-icon : disable
policy-object-in-dual-pane: disable
pre-login-banner : disable
private-data-encryption : disable
remoteauthtimeout : 10
search-all-adoms : disable
ssl-low-encryption : enable
ssl-protocol : tlsv1.3 tlsv1.2
ssl-static-key-ciphers: enable
table-entry-blink: enable
task-list-size : 2000
timezone : (GMT-8:00) Pacific Time (US & Canada).
tunnel-mtu : 1500
usg : disable
webservice-proto : tlsv1.3 tlsv1.2
```

system ha

Use this command to view HA configuration.

Syntax

```
get system ha
```

system interface

Use these commands to view interface configuration and status.

Syntax

```
get system interface
get system interface [interface name]
```

Examples

This example shows the output for `get system interface`:

```
== [ port1 ]
name: port1 status: enable ip: 111.11.11.11 255.255.255.0 speed: auto
== [ port2 ]
name: port2 status: enable ip: 0.0.0.0 0.0.0.0 speed: auto
== [ port3 ]
name: port3 status: enable ip: 0.0.0.0 0.0.0.0 speed: auto
== [ port4 ]
name: port4 status: enable ip: 0.0.0.0 0.0.0.0 speed: auto
```

This example shows the output for `get system interface port1`:

```
name : port1
status : enable
ip : 111.11.11.11 255.255.255.0
allowaccess : ping https ssh snmp soc-fabric http webservice fgfm
speed : auto
description : (null)
alias : (null)
mtu : 1500
type : physical
ipv6:
  ip6-address: ::/0 ip6-allowaccess: ip6-autoconf: enable
```

system locallog

Use these commands to view local log configuration.

Syntax

```
get system locallog disk filter
get system locallog disk setting
get system locallog [fortianalyzer | fortianalyzer2 |fortianalyzer3] filter
get system locallog [fortianalyzer | fortianalyzer2 |fortianalyzer3] setting
get system locallog memory filter
get system locallog memory setting
get system locallog setting
get system locallog [syslogd | syslogd2 | syslogd3] filter
```

```
get system locallog [syslogd | syslogd2 | syslogd3] setting
```

Examples

This example shows the output for `get system locallog disk setting`:

```
status : enable
severity : information
upload : disable
server-type : FTP
max-log-file-size : 100
max-log-file-num : 10000
roll-schedule : none
diskfull : overwrite
log-disk-full-percentage: 80
log-disk-quota : 5
```

This example shows the output for `get system locallog syslogd3 filter`:

```
controller : enable
event : enable
devops : enable
diskquota : enable
docker : enable
dvm : enable
ediscovery : enable
eventmgmt : enable
faz : enable
fazsys : enable
fmgws : enable
fortiview : enable
hcache : enable
incident: enable
iolog : enable
logd : enable
logdb : enable
logdev : enable
logfile : enable
logging : enable
report : enable
system : enable
```

system log

Use these commands to view log configuration.

Syntax

```
get system log alert
get system log device-disable
get system log fos-policy-stats
get system log interface-stats
get system log ioc
```

```
get system log mail-domain <id>
get system log ratelimit
get system log settings
get system log topology
```

Example

This example shows the output for `get system log settings`:

```
FAC-custom-field1 : (null)
FAZ-custom-field1 : (null)
FCH-custom-field1 : (null)
FCT-custom-field1 : (null)
FDD-custom-field1 : (null)
FGT-custom-field1 : (null)
FMG-custom-field1 : (null)
FML-custom-field1 : (null)
FPX-custom-field1 : (null)
FSA-custom-field1 : (null)
FWB-custom-field1 : (null)
browse-max-logfiles : 10000
device-auto-detect : enable
dns-resolve-dstip : disable
download-max-logs : 100000
ha-auto-migrate : disable
import-max-logfiles : 10000
keep-dev-logs : disable
log-file-archive-name: basic
rolling-regular:
sync-search-timeout : 60
unencrypted-logging : disable
```

system log-fetch

Use these commands to view log fetching configuration.

Syntax

```
get system log-fetch client-profile [id]
get system log-fetch server-settings
```

Example

This example shows the output for `get system log-fetch server-settings`:

```
max-conn-per-session: 3
max-sessions : 1
session-timeout : 10
```

system log-forward

Use this command to view log forwarding settings.

Syntax

```
get system log-forward [id]
```

system log-forward-service

Use this command to view log forward service settings.

Syntax

```
get system log-forward-service
```

Example

This example shows the output for `get system log-forward-service`:

```
accept-aggregation : enable
aggregation-disk-quota: 20000
```

system loglimits

Use this command to view log limits on your FortiAnalyzer unit.

Syntax

```
get system loglimits
```

Example

This example shows the output for `get system loglimits`:

```
GB/day : 250
Peak Log Rate : 10000
Sustained Log Rate : 4000
```

Where:

GB/day	Number of gigabytes used per day.
--------	-----------------------------------

Peak Log Rate	Peak time log rate.
Sustained Log Rate	Average log rate.

system mail

Use this command to view alert email configuration.

Syntax

```
get system mail [mail service id]
```

Example

This example shows the output for an alert email named `Test`:

```
id : Test
auth : disable
auth-type : psk
passwd : *
port : 25
secure-option : default
server : mailServer
user : mailperson@mailServer.com
```

system metadata

Use this command to view metadata settings.

Syntax

```
get system metadata admins [fieldname]
```

Example

This example shows the output for `get system metadata admins 'Contact Email'`:

```
fieldname : Contact Email
fieldlength : 50
importance : optional
status : enabled
```

system ntp

Use this command to view NTP configuration.

Syntax

```
get system ntp
```

Example

This example shows the output for `get system ntp`:

```
ntpserver:
  == [ 1 ]
  id: 1
  status : enable
```

system password-policy

Use this command to view the system password policy.

Syntax

```
get system password-policy
```

Example

This example shows the output for `get system password-policy`:

```
status : enable
minimum-length : 8
must-contain : upper-case-letter lower-case-letter number non-alphanumeric
change-4-characters : disable
expire : 60
```

system performance

Use this command to view performance statistics on your FortiAnalyzer unit.

Syntax

```
get system performance
```

Example

This example shows the output for `get system performance`:

```
CPU:
  Used: 100.00%
  Used(Excluded NICE): 100.00%
    %used %user %nice %sys %idle %iowait %irq %softirq
CPU0 100.00 100.00 0.00 0.00 0.00 0.00 0.00 0.00
Memory:
  Total: 4,134,728 KB
  Used: 2,105,988 KB 50.9%
Hard Disk:
  Total: 82,434,456 KB
  Used: 3,836,324 KB 4.7%
  IOStat: tps r_tps w_tps r_kB/s w_kB/s queue wait_ms svc_ms %util sampling_sec
          1.4 0.1 1.4 1.3 22.8 0.0 4.8 2.4 0.3 448240.73
Flash Disk:
  Total: 499,656 KB
  Used: 112,312 KB 22.5%
  IOStat: tps r_tps w_tps r_kB/s w_kB/s queue wait_ms svc_ms %util sampling_sec
          0.0 0.0 0.0 0.0 0.0 0.0 2.8 0.9 0.0 448240.82
```

system report

Use this command to view report configuration.

Syntax

```
get system report auto-cache
get system report est-browse-time
get system report group [group id]
get system report setting
```

Example

This example shows the output for `get system report setting`:

```
aggregate-report : disable
ldap-cache-timeout : 60
max-table-rows : 10000
report-priority : auto
template-auto-install: default
week-start : sun
```

system route

Use this command to view IPv4 routing table configuration.

Syntax

```
get system route [seq_num]
```

Example

This example shows the output for `get system route 66`:

```
seq_num : 66
device  : port5
dst     : 0.0.0.0 0.0.0.0
gateway : 10.111.1.16
```

system route6

Use this command to view IPv6 routing table configuration.

Syntax

```
get system route6 [seq_num]
```

system saml

Use this command to view SAML configuration.

Syntax

```
get system saml
```

Example

This example shows the output for `get system saml`:

```
status : enable
role   : SP
cert   : Fortinet_Local2
server-address : 172.27.2.225
login-auto-redirect : enable
entity-id : http://172.27.2.225/metadata/
acs-url   : https://172.27.2.225/saml/?acs
sls-url   : https://172.27.2.225/saml/?sls
idp-entity-id : http://http://172.27.2.224/saml-idp/sg45/metadata/
idp-single-sign-on-url: https://http://172.27.2.224/saml-idp/sg45/login/
idp-single-logout-url: https://http://172.27.2.224/saml-idp/sg45/logout/
idp-cert  : Remote_Cert_1
default-profile : Restricted_User
```

```
forticloud-sso : disable
user-auto-create : disable
```

system sniffer

Use this command to view the packet sniffer configuration.

Syntax

```
get system sniffer
```

system snmp

Use these commands to view SNMP configuration.

Syntax

```
get system snmp community [community ID]
get system snmp sysinfo
get system snmp user [SNMP user name]
```

Example

This example shows the output for `get system snmp sysinfo`:

```
contact_info : (null)
description : Test FAZ
engine-id : (null)
fortianalyzer-legacy-sysoid: disable
location : (null)
status : enable
trap-cpu-high-exclude-nice-threshold: 80
trap-high-cpu-threshold: 80
trap-low-memory-threshold: 80
```

system-soc-fabric

Use this command to view the SOC Fabric configuration.

Syntax

```
get system soc-fabric
```

Example

This example shows the output for `get system soc-fabric`:

```
status : disable
```

system sql

Use this command to view SQL configuration.

Syntax

```
get system sql
```

Example

This example shows the output for `get system sql`:

```
custom-index:
prompt-sql-upgrade : enable
status : local
text-search-index : disable
ts-index-field:
  == [ FGT-app-ctrl ]
  category: FGT-app-ctrl value:
    user,group,srcip,dstip,dstport,service,app,action,hostname
  == [ FGT-attack ]
  category: FGT-attack value: severity,srcip,dstip,action,user,attack
  == [ FGT-content ]
  category: FGT-content value: from,to,subject,action,srcip,dstip,hostname,status
  == [ FGT-dlp ]
  category: FGT-dlp value: user,srcip,service,action,filename
  == [ FGT-emailfilter ]
  category: FGT-emailfilter value: user,srcip,from,to,subject
  == [ FGT-event ]
  category: FGT-event value: subtype,ui,action,msg
  == [ FGT-traffic ]
  category: FGT-traffic value: user,srcip,dstip,service,app,utmaction
  == [ FGT-virus ]
  category: FGT-virus value: service,srcip,dstip,action,filename,virus,user
  == [ FGT-voip ]
  category: FGT-voip value: action,user,src,dst,from,to
  == [ FGT-webfilter ]
  category: FGT-webfilter value: user,srcip,dstip,service,action,catdesc,hostname
  == [ FGT-netscan ]
  category: FGT-netscan value: user,dstip,vuln,severity,os
  == [ FGT-fct-event ]
  category: FGT-fct-event value: (null)
  == [ FGT-fct-traffic ]
  category: FGT-fct-traffic value: (null)
  == [ FGT-fct-netscan ]
  category: FGT-fct-netscan value: (null)
```

```

== [ FGT-waf ]
category: FGT-waf value: user,srcip,dstip,service,action
== [ FGT-gtp ]
category: FGT-gtp value: msisdn,from,to,status
== [ FGT-dns ]
category: FGT-dns value: (null)
== [ FGT-ssh ]
category: FGT-ssh value: (null)
== [ FML-emailfilter ]
category: FML-emailfilter value: client_name,dst_ip,from,to,subject
== [ FML-event ]
category: FML-event value: subtype,msg
== [ FML-history ]
category: FML-history value: classifier,disposition,from,to,client_
      name,direction,domain,virus
== [ FML-virus ]
category: FML-virus value: src,msg,from,to
== [ FWB-attack ]
category: FWB-attack value: http_host,http_url,src,dst,msg,action
== [ FWB-event ]
category: FWB-event value: ui,action,msg
== [ FWB-traffic ]
category: FWB-traffic value: src,dst,service,http_method,msg
background-rebuild : enable
compress-table-min-age : 7
database-type : postgres
device-count-high : disable
event-table-partition-time: 0
fct-table-partition-time: 360
rebuild-event : enable
rebuild-event-start-time: 00:00 2000/01/01
start-time : 00:00 2000/01/01
traffic-table-partition-time: 0
utm-table-partition-time: 0

```

system status

Use this command to view the status of your FortiAnalyzer unit.

Syntax

```
get system status
```

Example

This example shows the output for `get system status`:

```

Platform Type : FAZ3000D
Platform Full Name : FortiAnalyzer-3000D
Version : v6.0.1-build0150 180606 (GA)
Serial Number : F-----2
BIOS version : 00010005

```

```
System Part-Number : P12907-03
Hostname : FAZ3000D
Max Number of Admin Domains : 4000
Admin Domain Configuration : Enabled
FIPS Mode : Disabled
Branch Point : 0150
Release Version Information : GA
Current Time : Tue Sep 29 08:09:05 PDT 2020
Daylight Time Saving : Yes
Time Zone : (GMT-8:00) Pacific Time (US & Canada).
x86-64 Applications : Yes
Disk Usage : Free 3083.01GB, Total 7332.97GB
File System : Ext4
```

system syslog

Use this command to view syslog information.

Syntax

```
get system syslog [syslog server name]
```

Example

This example shows the output for an syslog server named Test:

```
name : Test
ip : 10.10.10.1
port : 514
reliable : disable
```

system web-proxy

Use this command to view the system web proxy.

Syntax

```
get system web-proxy
```

Example

This example shows the output for `get system web-proxy`:

```
status : disable
mode : tunnel
address : (null)
port : 1080
```

get

```
username : (null)
password : *
```

show

The `show` commands display a part of your unit's configuration in the form of the commands that are required to achieve that configuration from the firmware's default state.



Although not explicitly shown in this section, for all `config` commands, there are related `show` commands that display that part of the configuration. The `show` commands use the same syntax as their related `config` command.



CLI commands and variables are case sensitive.

Unlike the `get` command, `show` does not display settings that are in their default state.

Example

```
FAZVM64 # show system global
config system global
    set adom-mode advanced
    set adom-status enable
    set hostname "FAZVM64"
end
```

Appendix A - Object Tables

Global object categories

38 "webfilter ftgd-local-cat"	47 "webfilter urlfilter"	51 "webfilter ftgd-local-rating"
52 "vpn certificate ca"	56 "spamfilter bword"	60 "spamfilter dnsbl"
64 "spamfilter mheader"	67 "spamfilter iptrust"	85 "ips custom"
140 "firewall address"	142 "firewall addrgrp"	255 "user adgrp"
145 "user radius"	146 "user ldap"	147 "user local"
148 "user peer"	152 "user group"	167 "firewall service custom"
254 "firewall service predefined"	168 "firewall service group"	170 "firewall schedule onetime"
171 "firewall schedule recurring"	172 "firewall ippool"	173 "firewall vip"
288 "ips sensor"	292 "log custom-field"	293 "user tacacs+"
296 "firewall ldb-monitor"	1028 "application list"	1038 "dlp sensor"
1043 "wanopt peer"	1044 "wanopt auth-group"	1054 "vpn ssl web portal"
1076 "system replacemsg-group"	1097 "firewall mms-profile"	1203 "firewall gtp"
1213 "firewall carrier-endpoint-bwl"	1216 "antivirus notification"	1327 "webfilter content"
1337 "endpoint-control profile"	1338 "firewall schedule group"	1364 "firewall shaper traffic-shaper"
1365 "firewall shaper per-ip-shaper"	1367 "vpn ssl web virtual-desktop-app-list"	1370 "vpn ssl web host-check-software"
1413 "webfilter profile"	1420 "antivirus profile"	1433 "spamfilter profile"
1472 "antivirus mms-checksum"	1482 "voip profile"	150 "system object-tag"
184 "user fortitoken"	273 "web-proxy forward-server"	335 "dlp filepattern"
343 "icap server"	344 "icap profile"	321 "user fsso"
390 "system sms-server"	397 "spamfilter bwl"	457 "wanopt profile"
384 "firewall service category"	474 "application custom"	475 "user device-category"
476 "user device"	492 "firewall deep-inspection-options"	800 "dynamic interface"
810 "dynamic address"	1004 "vpnmgr vpntable"	1005 "vpnmgr node"
1100 "system meta"	820 "report output"	822 "sql-report chart"
824 "sql-report dataset"	825 "sql-report dashboard"	827 "sql-report layout"

1494 "dynamic vip"	1495 "dynamic ippool"	1504 "dynamic certificate local"
1509 "dynamic vpntunnel"		

Device object ID values

1 "system vdom"	3 "system accprofile"	5 "system admin"
8 "system interface"	16 "system replacemsg mail"	17 "system replacemsg http"
18 "system replacemsg ftp"	19 "system replacemsg nntp"	20 "system replacemsg alertmail"
21 "system replacemsg fortiguard-wf"	22 "system replacemsg spam"	23 "system replacemsg admin"
24 "system replacemsg auth"	25 "system replacemsg im"	26 "system replacemsg sslvpn"
28 "system snmp community"	38 "webfilter ftgd-local-cat"	1300 "application recognition predefined"
47 "webfilter urlfilter"	51 "webfilter ftgd-local-rating"	52 "vpn certificate ca"
53 "vpn certificate local"	54 "vpn certificate cri"	55 "vpn certificate remote"
56 "spamfilter bword"	60 "spamfilter dnsbl"	64 "spamfilter mheader"
67 "spamfilter iptrust"	74 "imp2p aim-user"	75 "imp2p icq-user"
76 "imp2p msn-user"	77 "imp2p yahoo-user"	85 "ips custom"
117 "system session-helper"	118 "system tos-based-priority"	124 "antivirus service"
128 "antivirus quarfilepattern"	130 "system ipv6-tunnel"	314 "system sit-tunnel"
131 "system gre-tunnel"	132 "system arp-table"	135 "system dhcp server"
137 "system dhcp reserved-address"	138 "system zone"	140 "firewall address"
142 "firewall addrgrp"	255 "user adgrp"	145 "user radius"
146 "user ldap"	147 "user local"	148 "user peer"
152 "user group"	155 "vpn ipsec phase1"	156 "vpn ipsec phase2"
157 "vpn ipsec manualkey"	158 "vpn ipsec concentrator"	165 "vpn ipsec forticlient"
167 "firewall service custom"	254 "firewall service predefined"	168 "firewall service group"
170 "firewall schedule onetime"	171 "firewall schedule recurring"	172 "firewall ippool"
173 "firewall vip"	178 "firewall ipmacbinding table"	181 "firewall policy"
189 "firewall dnstranslation"	190 "firewall multicast-policy"	199 "system mac-address-table"
200 "router access-list"	202 "router aspath-list"	204 "router prefix-list"
206 "router key-chain"	208 "router community-list"	210 "router route-map"

225 "router static"	226 "router policy"	253 "system proxy-arp"
284 "system switch-interface"	285 "system session-sync"	288 "ips sensor"
292 "log custom-field"	293 "user tacacs+"	296 "firewall ldb-monitor"
297 "ips decoder"	299 "ips rule"	307 "router auth-path"
317 "system wccp"	318 "firewall interface-policy"	1020 "system replacemsg ec"
1021 "system replacemsg nac-quar"	1022 "system snmp user"	1027 "application name"
1028 "application list"	1038 "dlp sensor"	1041 "user ban"
1043 "wanopt peer"	1044 "wanopt auth-group"	1045 "wanopt ssl-server"
1047 "wanopt storage"	1054 "vpn ssl web portal"	1061 "system wireless ap-status"
1075 "system replacemsg-image"	1076 "system replacemsg-group"	1092 "system replacemsg mms"
1093 "system replacemsg mm1"	1094 "system replacemsg mm3"	1095 "system replacemsg mm4"
1096 "system replacemsg mm7"	1097 "firewall mms-profile"	1203 "firewall gtp"
1213 "firewall carrier-endpoint-bwl"	1216 "antivirus notification"	1326 "system replacemsg traffic-quota"
1327 "webfilter content"	1337 "endpoint-control profile"	1338 "firewall schedule group"
1364 "firewall shaper traffic-shaper"	1365 "firewall shaper per-ip-shaper"	1367 "vpn ssl web virtual-desktop-app-list"
1370 "vpn ssl web host-check-software"	1373 "report dataset"	1375 "report chart"
1382 "report summary"	1387 "firewall sniff-interface-policy"	1396 "wireless-controller vap"
1399 "wireless-controller wtp"	1402 "wireless-controller ap-status"	1412 "system replacemsg webproxy"
1413 "webfilter profile"	1420 "antivirus profile"	1433 "spamfilter profile"
1440 "firewall profile-protocol-options"	1453 "firewall profile-group"	1461 "system storage"
1462 "report style"	1463 "report layout"	1472 "antivirus mms-checksum"
1482 "voip profile"	1485 "netscan assets"	1487 "firewall central-nat"
1490 "report theme"	150 "system object-tag"	169 "system dhcp6 server"
180 "system port-pair"	182 "system 3g-modem custom"	183 "application rule-settings"
184 "user fortitoken"	212 "webfilter override"	270 "firewall local-in-policy"
273 "web-proxy forward-server"	330 "system ddns"	331 "system replacemsg captive-portal-dflt"
335 "dlp filepattern"	337 "dlp fp-sensitivity"	338 "dlp fp-doc-source"
342 "webfilter ftgd-warning"	343 "icap server"	344 "icap profile"

352 "system monitors"	354 "system sp"	321 "user fsso"
355 "router gwdetect"	386 "system physical-switch"	388 "system virtual-switch"
390 "system sms-server"	394 "system replacemsg utm"	397 "spamfilter bwl"
406 "vpn certificate ocsp-server"	408 "user password-policy"	412 "webfilter search-engine"
428 "firewall identity-based-route"	431 "web-proxy debug-url"	432 "firewall ttl-policy"
434 "firewall isf-acl"	435 "firewall DoS-policy"	437 "firewall sniffer"
438 "wireless-controller wids-profile"	439 "switch-controller vlan"	441 "switch-controller managed-switch"
453 "firewall ip-translation"	457 "wanopt profile"	269 "firewall multicast-address"
384 "firewall service category"	466 "system ips-urlfilter-dns"	467 "system geoip-override"
474 "application custom"	475 "user device-category"	476 "user device"
483 "system server-probe"	473 "system replacemsg device-detection-portal"	492 "firewall deep-inspection-options"

Appendix B - CLI Error Codes

Some FortiAnalyzer CLI commands issue numerical error codes. The following table lists the error codes and descriptions.

Error Code	Description
0	Success
1	Function called with illegal parameters
2	Unknown protocol
3	Failed to connect host
4	Memory failure
5	Session failure
6	Authentication failure
7	Generic file transfer failure
8	Failed to access local file
9	Failed to access remote file
10	Failed to read local file
11	Failed to write local file
12	Failed to read remote file
13	Failed to write remote file
14	Local directory failure
15	Remote directory failure



www.fortinet.com

Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.